



D3.7 EU White Paper around legal compliance and policy statements including recommendations

Author(s)	ICT Legal Consulting
Status	Final
Version	1.0
Date	30/07/2021

Dissemination Level

<input checked="" type="checkbox"/>	PU: Public
<input type="checkbox"/>	PP: Restricted to other programme participants (including the Commission)
<input type="checkbox"/>	RE: Restricted to a group specified by the consortium (including the Commission)
<input type="checkbox"/>	CO: Confidential, only for members of the consortium (including the Commission)

Abstract:

This deliverable ("Deliverable") offers recommendations to policymakers with regards to the legal compliance of stakeholders with the General Data Protection Regulation and the Directive on security of network and information systems. The progress made in the past years and the challenges remaining are presented. The challenges brought about by the deployment of new technologies like Artificial Intelligence, and Internet of Things together with recommendations will also be offered, with the aim of providing useful insights in the topics that will require attention by policy makers and Supervisory Authorities in the near future. Finally, the Deliverable provides also legal recommendations on privacy and cybersecurity to the two stakeholders of Cyberwatching.eu, small and medium enterprises, in order to enhance their legal compliance posture.



The work described in this document has been conducted within the project cyberwatching.eu. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 740129. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

Document identifier: Cyberwatching.eu – WP 3 – D3.7	
Deliverable lead	ICTL Legal Consulting
Related work package	WP3
Author(s)	Paolo Balboni, Anastasia Botsi, Laura Senatore, ICT Legal Consulting
Contributor(s)	-
Due date	31/07/2021
Actual submission date	30/07/2021
Reviewed by	Paolo Modica, AON; Justina Beiliauskaite & James Philpot, DSME; Nicholas Ferguson, Trust-IT
Start date of Project	01/05/2017
Duration	51 months

Revision history

Version	Date	Authors	Notes
v0.1	09.07.2021	Paolo Balboni, Laura Senatore, and Anastasia Botsi (ICTLC)	Drafting of Deliverable and sharing with the Consortium
V0.2	19.07.2021	Paolo Balboni, Laura Senatore, and Anastasia Botsi (ICTLC)	Finalising sections on emerging technologies, Abstract, Executive Summary and Summary of Recommendations and sending it to reviewers
V0.3	27.07.2021	Paolo Modica (AON), and Justina Bieliauskaite	Full document internal review and comment
V0.4	28.07.2021	Paolo Balboni, Laura Senatore, and Anastasia Botsi (ICTLC)	Address feedback by peer reviewers, fix formatting issues.
V1.0	30.07.2021	Nicholas Ferguson (Trust-IT)	Final version and PMB review

Executive Summary

The work in this deliverable is related to Objective 3 of cyberwatching.eu, which is to “play a supporting role in the policy, regulatory standards & legal discussions that contribute to shaping up the global cybersecurity & privacy landscape.”

This document is the White paper around legal compliance & policy statements including recommendations (M51), which is the final version of a preliminary version D3.4 (M26) relating to the Task 3.4 on Legal Compliance in cybersecurity & privacy. It combines the legislation, the best practices available, the guidelines or opinions of the European Data Protection Supervisor (“EDPS”)¹, the European Data Protection Board (“EDPB”, former Article 29 Working Party)², the High Level Expert Group of Artificial Intelligence (“HLEG AI”)³, as well as of competent Supervisory Authorities (“SAs”) of EU Member States, and the practical considerations of European Projects (“EU Projects”), and Small and Medium Enterprises (“SMEs”) participating at the various stakeholders’ events throughout the duration of the Cyberwatching.eu project. The document offers a robust package of recommendations facing both the policy makers and the Supervisory Authorities, to address stakeholders’ needs. Clear explanations of the fundamental obligations included in the EU Regulation 2016/679, known as “General Data Protection Regulation” or “GDPR”, can best be provided by the experts that practice and apply the GDPR on a day-to-day basis, making the cyberwatching.eu partners the most appropriate resource of creating this impact. The ultimate aim of merging the legal knowledge and practical observation of reality was to develop online tools that are meant to complement one another, resulting in self-assessment tools that provide handy self-explanatory legal and practical recommendations for all stakeholders, including SMEs. The legal online tools (GDPR Temperature Tool⁴ and Information Notice Tool⁵) have been significantly revamped since D3.4, including new functions such as the embedding of services and products created by Research and Innovation projects (“R&I projects”) to immediately recommend tools that can assist in the compliance of SMEs with legal requirements.

Cyberwatching.eu offers a platform where the extensive community can be engaged, for example through the yearly Concertation meetings that are organised for R&Is, or via the SMEs joining policy discussions. Cyberwatching.eu also helps the dissemination of other EU Projects and R&Is in general, by means of promoting among the cyberwatching.eu stakeholders (i.e., the SMEs) the solutions of R&Is. In this context, the new versions of the tools are an innovative way to promote these solutions.

The focus of this White Paper is to highlight the progress made since D3.4 and the remaining challenges for the cyberwatching.eu’s stakeholders on the topic of legal compliance. Seeing as cyberwatching.eu is the European watch on cybersecurity & privacy, many stakeholders are either developing or deploying emerging technologies, and this is the main reason why the scope of the legal challenges and legal

¹ The European Data Protection Supervisor is the European Union’s independent data protection authority. More information is available at: https://edps.europa.eu/_en.

² The European Data Protection Board is an independent European Body contributing to the consistent application of data protection rules throughout the European Union, and promotes the consistent application between the various national supervisory authorities. More information is available at: https://edpb.europa.eu/edpb_en.

³ The European Commission has appointed the High-Level Expert Group on Artificial Intelligence, which is a group of 52 experts representing different stakeholders, such as Academia, civil society and the industry, from the Academia, civil society, as well as industry with the purpose of implementing the European Agency on Artificial Intelligence. More information is available at: <https://www.ai4eu.eu/>.

⁴ Available at: <https://gdprtool.cyberwatching.eu/Pages/Home.aspx>.

⁵ Available at: <https://infonoticeitool.cyberwatching.eu/Pages/Home.aspx>.

recommendations provided tackle the two emerging technologies of Artificial Intelligence and Internet of Things.

The aim of the legal recommendations is twofold: firstly, to give insight to stakeholders of how they can overcome these challenges, and, secondly, to provide policy makers and enforcement authorities with suggestions on how to assist these stakeholders in their journey to compliance.

The main recommendations from the White Paper are listed below and are discussed throughout the document and summarised fully in section six.

Recommendations on GDPR:

- a) *Creation of a single space to collect all the different types of guidance (opinions, guidelines, instruments, tools, self-assessments) created by Supervisory Authorities based on the GDPR 'topic' or GDPR 'obligation' to ensure easy access availability.*
- b) *Publication of a systematic Methodology for GDPR risk assessments which will be available for all stakeholders in every Member State.*
- c) *Allocation of specific priority areas that require instruments or guidance to different Supervisory Authorities, in order to ensure efficiency and consistency in the guidance provided to organisations.*
- d) *Updated methodology to assess the severity of data breaches and feedback on tool for notification of data breaches by modernizing of the existing methodology from ENISA.*
- e) *European tool for Data Protection Impact Assessment which could compile the several applicable national "black lists".*
- f) *Publication of guidelines and recommendations on Data Transfer Impact Assessment.*
- g) *Creation of a data transfer impact assessment, which will assist organisations to assess all relevant factors and considerations before carrying out data transfers outside the EEA.*
- h) *Further research on managing notifications that fulfill the requirements of both the NISD and the GDPR.*

Recommendations on emerging technologies:

- a) *Creation of practical tools focusing on compliance of emerging technologies, that are kept up to date according to the industry standards and state of art as well as rate of change of the technologies.*
- b) *Creation of a distinct methodology for development and deployment of emerging technologies in order to support the European research & innovation projects.*
- c) *Education and training to raise industry awareness in the field of emerging technologies.*
- d) *Structured cooperation between policy makers, the research and the market/industry.*

Recommendations on Artificial Intelligence

- a) *Guidelines on the methodology for risk analysis relating to all levels of risk of AI, aiming at further clarifying the ever-changing aspects of AI.*
- b) *Guidelines on AI/machine learning and data minimisation*
- c) *Provide clarification, through the Artificial Intelligence Act, the tensions between the GDPR principle of purpose limitation and the training and deployment of AI systems*
- d) *Provide guidance on the methodology that SMEs / start-ups training or implementing AI systems in their processes should follow.*

- e) *Guidance and/or other means for AI developers and users to have the ability to provide dynamic information notices (using illustrations, flowcharts, videos, etc.).*
- f) *Guidance around the requirement of traceability as introduced by the High-Level Expert Group on Artificial Intelligence.*
- g) *Provide opportunities to research initiatives, through the Horizon Europe or Digital Europe Program, to explore further ways to grant transparency – for data subjects – on the logic of the automated processing which regards them.*
- h) *Development of further clear and understandable guidelines for AI developers and users on (1) AI risk management, and (2) examples of security measures, at varying levels of sophistication which may be considered to properly address identified risks.*
- i) *Further research and the development of clear, understandable and practical guidelines developing the concept of Fairness by Design (a checklist which could be relied on by AI-based solution developers).*

Recommendations on Internet of Things:

- a) *Need for further guidelines on the application of principles of data protection by design/default and data minimisation for IoT deployments.*
- b) *Practical guidelines on the allocation of privacy roles in IoT environments in the light of the GDPR.*
- c) *Guidance or further research into the key aspects to be regulated between stakeholders, via Data Management Agreements (in particular, where the controller-to-controller terms are concerned), to provide tools for stakeholders to effectively self-regulate.*
- d) *Impose limitations or further requirements on subsequent processing of personal data, collected and shared between IoT-connected devices and services.*
- e) *Guidelines on effective means by which information on processing activities carried out via IoT can be delivered to individuals – particular those who may be captured by the sensors of such devices, without necessarily owning them or having activated them (such as visitors or passers-by).*
- f) *Guidelines and procedures to assist controllers in carrying out regular monitoring and testing activities, when faced with systems composed of multiple IoT-connected devices.*
- g) *Ensure that IoT developers and users are bound by ethical considerations in their activities, further research and the development of clear, understandable and practical guidelines developing the concept of Fairness by Design (including, for example, a checklist which could be relied on by IoT-based solution developers) would be welcomed.*

Table 1 Main recommendations listed

Table of Contents

1	Introduction.....	7
2	Legal Compliance: GDPR Challenges and Recommendations	9
2.1	Compliance with the GDPR: SMEs, research projects, emerging technologies.....	9
2.1.1	Progress made	10
2.1.2	Remaining challenges	14
2.2	Compliance of Emerging Technologies	18
2.3	Artificial Intelligence (AI).....	21
2.3.1	Progress made	21
2.3.2	Challenges remaining	25
2.4	Internet of Things (IoT).....	35
2.4.1	Challenges remaining	36
3	The fourth Concertation Meeting 2021	45
4	GDPR Temperature Tool 2.0, Information Notice Tool 2.0 and Interactive Webinar with SMEs.....	47
5	SUMMARY OF RECOMMENDATIONS	48
	ANNEXES	51
Annex A.	Survey and recommendations for SMES: the GDPR temperature tool 52	
Annex B.	Survey and recommendations for information notices	89
Annex C.	Presentation slides for GDPR webinar.....	101
Annex D.	Participation at Legal compliance webinars, workshops, round-table discussions, panels.....	116
Annex E.	R&I Solutions index.....	118
Annex F.	Glossary	128
 TABLE OF TABLES		
Table 1	Main recommendations listed.....	5
Table 2	Legal compliance webinars, workshops, roundtables discussions, panels ...	117

1 Introduction

This document demonstrates the specific activities that have been conducted throughout the past years and delivers practical insights from the cluster effort around EU R&I teams, particularly by going over the policy evolution, the progress made, and the challenges in the efforts of implementing cybersecurity and privacy into the society.

The goal is to offer a supporting role between the regulatory framework that has been implemented within the EU and the market that needs to apply it to the activities it carries out.

The previous deliverables (D3.4⁶, D4.4⁷) linked to task 3.4 have already tackled the general intricacies between the [Regulation \(EU\) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC](#) (hereinafter “GDPR”) and the [Directive \(EU\) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union](#) (hereinafter “NISD”). This White Paper’s scope is different and aims to take a critical standpoint in presenting the challenges that have emerged in the legal compliance posture of stakeholders, such as EU projects and SMEs, both with the GDPR and the NISD. These challenges have been collected through various ways. Firstly, they are the result of consistent monitoring of the legal landscape and research on the challenges pointed out by advocacy groups, alliances, and consortiums. In addition, an ongoing discussion between the legal experts of the consortium and cyberwatching.eu stakeholders through webinars, roundtables, workshops, panel discussions, Concertation Meetings, face-to-face meetings, were a catalyst to observing the practical obstacles to legal compliance. Lastly, the GDPR Temperature Tool – an online self-assessment tool providing customisable legal recommendations to organisations regarding their GDPR compliance posture – helped to create a realistic overview of the main topics that organisations, mainly SMEs, have gaps in their legal compliance.

As a result, this White Paper analyses the challenges to legal compliance, clarifies what has been done so far on these challenges, and recommends remaining actions that can be taken, either by policy makers, by Supervisory Authorities, or by the European Data Protection Board (“EDPB”) in order to assist the stakeholders in their journey to legal compliance. Further, the Consortium has also created its own tools to help increase the legal compliance of its stakeholders, namely, the GDPR Temperature Tool⁸ and the Information Notice Tool.⁹ These tools provide a specific legal recommendation to organisations, depending on what obligations they have yet complied with. In addition, the legal recommendations included in the tools also integrate the R&I solutions that were deemed appropriate to assist an SME in their legal compliance activities. By bringing forward these multi-faceted recommendations, the Consortium aims to help save costs and encourage innovative organisations to transform privacy and cybersecurity challenges in opportunities to increase their competitiveness.

In section two, the legal compliance with regards to the GDPR will be presented, in order to state the progress made and the remaining challenges, in order to help policy-

⁶ Available at: <https://www.cyberwatching.eu/publications/eu-cybersecurity-legal-and-policy-aspects-preliminary-recommendations-and-road-ahead>.

⁷ Available at: <https://www.cyberwatching.eu/d44-eu-cybersecurity-privacy-interim-roadmap>

⁸ Available at: <https://gdprtool.cyberwatching.eu/Pages/Home.aspx>.

⁹ Available at: <https://infonoticeetool.cyberwatching.eu/Pages/Home.aspx>.

makers, Supervisory Authorities, and the EDPB to identify the topics that require further attention in the near future. Following this, an in-depth discussion of the data protection challenges that are posed by the development and deployment of Artificial Intelligence (“AI”) and Internet of Things (“IoT”) is provided. The aim of this section is to raise the awareness of legislators on the possible issues that may be inherent to the processing of personal data by means of these technologies and suggest ways with which to solve the potential conflicts between compliance and innovation. This section also provides practical insights on challenges for AI systems that the policy-makers can rely on, in order to actively engage in the discussions around the Artificial Intelligence Act (“AIA”) proposal.

The third section complements the above results, by providing the most up to date discussion on the challenges emerging technologies pose to privacy and data protection through an overview of the third Concertation Meeting which took place on 13th July 2021.

The fourth section is created for the stakeholders of cyberwatching.eu. On the one hand, the updated content of the GDPR temperature tool for EU Projects and SMEs which has been published and converted into an online tool on the cyberwatching.eu web platform and promoted to SMEs will be presented. This has been generated as a preliminary step for SMEs to facilitate their understanding of where they stand with respect to the GDPR in terms of “risks to sanctions”. This is not an attempt, nor is it supposed to be replaced by the risk assessment that should be conducted by SMEs (i.e., risks of varying likelihood and severity for rights and freedoms of natural persons posed by the relevant processing activities), but merely an indication of their risk to sanctions, according to their responses which provide a basis of their processing activities. Therefore, this tool is to be used as recommendations to organisations on how to have a more GDPR compliant posture. This tool was also complemented by an interactive webinar between the legal experts and the SMEs that completed the tools, in order to share the overall status of compliance, give additional recommendations, and receive feedback on the tools themselves. In summary, these activities have been carried out so as **to effectively enable all stakeholders focused on privacy and cybersecurity to participate in the policy-making debate, both at national and EU levels, on these matters.**

Section five of this Deliverable includes a summary of all the recommendations.

2 Legal Compliance: GDPR Challenges and Recommendations

Legal compliance these days involves multiple factors, not only the understanding and implementation of the current legislation on a European and national level but also the preparation of the organisations and employees to further compliance by way of staying up to date with the latest proposals, legal debates, opinions, and approaches that are available. In order to present a full picture of the current legal compliance and policy statements, this chapter will first present the progress made and remaining challenges in legal compliance on the GDPR, and the NISD. This aims to help SMEs or Research and Innovation Projects to understand where they stand with regards to legal compliance, and also inform themselves of the most challenging topics.

Understanding the main challenges in compliance will not only help solve potential conflicts of interpretation but will also enable cyberwatching.eu stakeholders focused on privacy and cybersecurity to effectively participate in the policy-making debate of the next years, both at the national and EU level, on these matters.

The main purpose of highlighting these challenges is to come up with recommendations that will be facing the policy makers – in order to both clarify areas that are ambiguous or can appear problematic in the compliance of stakeholders. This section will be a more critical component in the interplay of the different future legislations, that will serve as suggestions or clarifications to policy makers.

Seeing as the two legislations of the GDPR and NISD have been briefly introduced in previous deliverables (specifically, D3.2 EU cybersecurity and privacy R&I ecosystem, D3.3 White paper on cybersecurity standard gap analysis, and D3.4 EU Cybersecurity legal and policy aspects: preliminary recommendations and road ahead), we will only provide an overview of those challenges that still exist. Once this is done, we will propose the areas that seem to require further elucidation, further guidance, or more specific regulation in order to ensure the legal compliance of cyberwatching.eu stakeholders. As a preliminary remark, the GDPR is analysed more in depth due to its widespread applicability; meanwhile, the NISD will be discussed in a short section, since it is more strictly focused on the essential services of each Member State – therefore its scope is inevitably more limited.

Finally, an in-depth analysis of the challenges posed to legal compliance on emerging technologies, such as Artificial Intelligence and Internet of Things will be presented, following up on the previous preliminary recommendations of D3.4. It is worth noting that apart from the two legislations that will be discussed in this deliverable, the European Commission has already proposed a text for the Artificial Intelligence Act. This goes to show that the near future will bring further transformations of the legal system to ensure consistency, less legal uncertainty and an evolvement of the law which can regulate the market more comprehensively and effectively. These developments will be also pointed out, as well as any other guidance that can help stakeholders of cyberwatching.eu to take the role in helping the legislation be communicated in a straightforward manner throughout the different fields that it applies to, and as a result point to policy-makers areas that may need further clarification and/or guidance from the EU level.

2.1 Compliance with the GDPR: SMEs, research projects, emerging technologies

The European Data Protection Board has recently published their Annual Report for 2020, which summarises both the highlights of the General Data Protection Regulation but also the challenges with its implementation, enforcement and comprehension.

Overall, the harmonisation of interpretation of data protection principles seems to have strengthened the compliance of companies and the reinforcement of data subject rights.¹⁰ The GDPR is considered a role model data protection legislation globally¹¹, which increases the competitive advantage of SMEs and organisations when it comes to respecting privacy and providing data protection to their customers and clients. Nevertheless, some aspects remain unsolved or, at least, not practically clarified, which calls for companies to coming up with innovative solutions to overcome them. Although some organisations have the capacity to find such solutions, many have neither the expertise nor the financial resources to address these challenges on their own. According to TrustArc, only 20% of businesses believe they are GDPR compliant, while more than 1 in 4 companies (around 27%) have not even initiated their efforts towards GDPR compliance in 2019.¹²

In a blog post for the three-year anniversary of the GDPR, Wojciech Wiewiórowski, the European Data Protection Supervisor, encouraged data protection authorities to make use of all the powers in their regulatory toolbox in order to apply the law and protect citizens.¹³ Mr. Wiewiórowski pushes authorities to increase the enforcement actions especially towards the “giant players” that cause systemic harm in the digital ecosystem. However, strict enforcement may also act as a deterrent and even punishment for the SMEs that desperately try to keep up with all the legislations concerning data protection, privacy and cybersecurity.

Therefore, this chapter has collected the challenges posed to SMEs, research projects, and developers or providers of emerging technologies (such as Artificial Intelligence, and Internet of Things,) in achieving legal compliance. This chapter tackles both the more generic challenges to legal compliance, while also addressing the challenges posed to emerging technologies. The aim is to ensure that regulatory gaps are filled but also that SMEs receive the appropriate tools in support of their compliance efforts.

2.1.1 Progress made

In the preliminary deliverable 3.4 on *Cybersecurity legal and policy aspects: preliminary recommendations and road ahead*, a set of challenges were identified, accompanied by recommendations for policy makers, agencies, and enforcement authorities. In the past years, progress has been made with regards to these challenges, helping close the gap between compliance theory and company practices. This sub-section aims to highlight the areas in which progress has been made, to recognise the advancements made to support SMEs and other stakeholders and have a more accurate picture of the reality stakeholders face for achieving legal compliance. In addition, these highlights of progress can help identify further actions of improvement on these areas.

¹⁰ 2020 Annual Report Ensuring Data Protection Rights in a Changing World 2020, European Data Protection Board, p.16, available at: https://edpb.europa.eu/our-work-tools/our-documents/annual-report/edpb-annual-report-2020_en.

¹¹ 2020 Annual Report Ensuring Data Protection Rights in a Changing World 2020, European Data Protection Board, p.16, available at: https://edpb.europa.eu/our-work-tools/our-documents/annual-report/edpb-annual-report-2020_en.

¹² Report benchmarks GDPR compliance status post May 25th deadline for US and EU companies, EU GDPR Research Report, available at: https://edpb.europa.eu/our-work-tools/our-documents/annual-report/edpb-annual-report-2020_en.

¹³ GDPR: a three-year-old who must still learn to walk before it runs, Wojciech Wiewiórowski, European Data Protection Supervisor, available at: https://edps.europa.eu/press-publications/press-news/blog/gdpr-three-year-old-who-must-still-learn-walk-it-runs_en.

2.1.1.1 Methodology for GDPR risk assessments

The first recommendation from D3.4 was the publication of a systematic methodology, or even a tool, for GDPR risk assessments. This recommendation has recently been met by the Spanish Data Protection Authority (AEPD) through the publication of a new guide on risk management and carrying out Data Protection Impact Assessment.¹⁴ This new tool collects the interpretations of the AEPD, the EDPB, and the EDPS and its very aim is to help data controllers, and processors in their compliance efforts with this obligation. Together with this guidance, the AEPD has put forth its 'Evaluate-Risk GDPR tool' which is a practical tool for i) identifying risks posed to the rights and freedoms of data subjects in processing activities, ii) carrying out a first assessment of the risk (including a Data Processing Impact Assessment), iii) estimating the residual risk, after applying measures and guarantees for risk mitigation. This action fulfils the recommendation given by the previous deliverable and requested at multiple times from stakeholders. However, its limitation is that it is only provided in Spanish language.

The nature of the European Union having local legislation and local data protection authorities may at times call for consistency in ensuring that certain tools are available widely throughout the entire EU in order for all stakeholders to benefit from. As a result, although progress has been made on this topic, an additional recommendation can be provided when considering the new legislative initiatives that will be proposed in the upcoming years. The recommendation for policy makers to consider is to **encourage the EDPB or the European Commission to monitor tools, open-source software and other practical instruments that have been provided by Data Protection Authorities and ensure that they are available for the entire European Digital Single Market.**

The amount of effort required can consist of a mere translation of such tools, or even 'localise' them with the help of the relevant national Supervisory Authority (SA). This will, on the one hand, be a more efficient allocation of efforts and resources of the different SAs. Such an approach could consist of one or two Supervisory Authorities taking a leading role or prioritising the creation of practical instruments on a certain area, while the others address the national considerations.¹⁵ By implementing this approach, the SAs will all focus on developing tools in the different challenging topics of implementation for organisations, which will be widely distributed around the EU data protection authorities; while other SAs will not be required to spend substantial number of resources on the exact same areas. In addition, this is a reasonable approach which can support the smaller SAs that may not have as many resources, personnel, or capabilities as others. Finally, it can also support and guarantee a consistency in application of the GDPR requirements and ensure that all important aspects are duly taken into account. Implementing this recommendation would be ideal for cyberwatching.eu's stakeholders, especially for companies that do not have the

¹⁴ Gestión del riesgo y evaluación de impacto en tratamientos de datos personales, Agencia Española Protección Datos, June 2021, <https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf>.

¹⁵ In doing so, the SAs can also distribute the development of the practical instruments and tools, according and to the extent of the expertise that each authority has. A recent report published by an advocate group Access Now came to worrisome conclusions when reviewing the two-year application of the GDPR (Available here: <https://www.accessnow.org/cms/assets/uploads/2020/05/Two-Years-Under-GDPR.pdf>); concluding that there are insufficient resources, minimal budgets and administrative complications in the enforcement of the GDPR. This report further strengthens the argument that Supervisory authorities must collaborate and use their limited sources as efficiently as possible. For this to take place, SAs must join forces both when it comes to enforcing the GDPR and imposing fines, as well as in providing opinions and guidelines to organizations.

personnel nor resources to adapt their assessments according to the different national tools.

2.1.1.2 European self-assessment toolkits

The second progress made is on the aspect of European self-assessment toolkits, which aim to help ‘translate’ the principles, requirements, and obligations of the GDPR. This recommendation was reiterated frequently in cyberwatching.eu’s Concertation Meeting in 2019.¹⁶ Although a broadly used single European self-assessment has not been produced, many efforts to create practical tools can be noticed.

Firstly, the nearest tool of self-assessments is the “toolkit” by the Information Commissioner’s Office (“ICO”) addresses these challenges at national level, including a Data Protection self-assessment checklist on topics that they deemed to be crucial to improve the data protection compliance of data controllers and processors, especially for the small and medium-sized organisations.¹⁷ Further, ENISA has provided two different useful practical tools on different areas for the security of personal data processing. Initially, the risk assessment tool for carrying out risk assessments aiming to guide SMEs through their specific data processing activities and helping them evaluate the relevant security risks.¹⁸ The advantage of this tool is that it builds on the existing tools such as the CNIL’s methodology for privacy risk management, ENISA’s recommendation for a methodology of the assessment of severity of personal data breaches, and ENISA’s Risk Management and Risk Assessment for SMEs pilot study. In addition to the risk assessment, ENISA published an online tool that helps organisations identify the security measures appropriate to the level of risk and the type of processing activity at hand.¹⁹ These two self-assessment tools can be used together for organisations to firstly assess the risk to the processing of personal data and then compare that risk with ENISA’s methodology in identifying the corresponding implemented security measures.

Finally, ENISA also provided a practical tool for the implementation of the good practices in healthcare services. This tool aims to assist hospitals assess the cybersecurity requirements for services, products and infrastructures procured in this sector.²⁰ The health-care sector is one of the essential services identified by the NISD, and hence is an exemplar tool for the other essential service providers sectors.

It is clear from the above that progress has been made with regards to available tools providing a self-assessment on GDPR or NISD requirements. However, even knowing that these tools exist and collating them from the different national Supervisory Authorities is a challenge. Therefore, it is important to reiterate the core of the recommendation from D3.4 for future European research & Innovation projects to create a **pan-European self-assessment tool taking into consideration the European perception as well as the expertise and decisions coming from the different member states’ Supervisory Authorities**. Should this not be possible, the EDPB can aim to **collect all the different guidelines, instruments, and tools**

¹⁶ More information on the second concertation meeting available at: <https://www.cyberwatching.eu/news-events/events/brussels-second-cw-concertation-meeting-04062019-0>.

¹⁷ Information Commissioner's Office Data protection self assessment, Available at: <https://ico.org.uk/for-organisations/data-protection-self-assessment/>.

¹⁸ Evaluating the level of risk for a personal data processing operation, Available at: <https://www.enisa.europa.eu/risk-level-tool/risk>.

¹⁹ (Self)assessing the implemented security measures, Available at: <https://www.enisa.europa.eu/risk-level-tool/assessment>.

²⁰ Good practices for the security of healthcare services, Available at: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/health/good-practices-for-the-security-of-healthcare-services#.

created by Supervisory Authorities per GDPR ‘topic’ or per GDPR ‘obligation’ – that way all tools available are collected in one single space and stakeholders such as SMEs will not need to look into the activities of every single SA in order to find useful guidance. In addition, the online tool created by ENISA to assist hospitals can be **replicated for other sectors as well, such as transport, and energy, in order to further assist these essential services, improve their cybersecurity in a consistent and practical way.**

2.1.1.3 Updated methodology for severity of data breaches assessments and methodology to manage breaches

In the Second Concertation Meeting stakeholders recommended the importance of providing further guidelines on the assessment of the severity of personal data breaches, which relies on the risk-based approach. In addition, a methodology managing and reacting to the breaches was suggested, such as “guidelines on the implementation of appropriate measures to prevent the breaches, as well as the provision of a structured approach on assessing and mitigating risks”.²¹ The recommendation is especially important for emerging technologies, since the surface devices and volumes of data can leave an organisation vulnerable both from the perspective of preventing personal data breaches, as well as mitigating them, through security measures.

Although the update to the methodology for severity of data breach assessments was identified as a “short-term” recommendation in the preliminary deliverable (D3.4), relatively little progress has been made to provide an exclusive methodology for assessing the severity of data breaches. In the beginning of 2021, the European Data Protection Board published the Guidelines on Examples regarding Data Breach Notifications which provides guidelines in practical issues in more details. The document aims to help data controllers in generally handling data breaches and understanding the factors that should be considered during the risk assessment.²² These Guidelines cover the first layer of the recommendation given by cyberwatching.eu stakeholders, as they present typical cases of data breaches and how they must be analysed, assessed, and notified to the SAs. Stakeholders could use these data breach ‘cases’ to get a general understanding of what is expected to be done when a specific breach occurs, however, they do not provide a complete and concrete methodology for assessing the severity of data breaches. As a result, **only the first level of this recommendation has been fulfilled, as the EDPB has provided a useful first approach in how organisations should handle the most common data breaches.** Since the stakeholders of cyberwatching.eu are SMEs, R&I projects, and other organisations, it is reasonable to assume that the most frequent cases will occur to them, such as a ransomware, an internal human error, or an accidental transmission of data to a trusted third party. These guidelines were an important step to assisting SMEs achieve a higher level of compliance with regards to data breaches. Nevertheless, the gap remains since organisations must extract information from the practical examples instead of relying on a structured approach for their severity assessments. Therefore, **a concrete update to the severity**

²¹ D3.4 EU Cybersecurity legal and policy aspects: preliminary recommendations and road ahead, p. 28, Available at: <https://cyberwatching.eu/d34-eu-cybersecurity-legal-and-policy-aspects-preliminary-recommendations-and-road-ahead>.

²² Guidelines 01/2021 on Examples regarding Data Breach Notification, Adopted on 14 January 2021, Version 1.0, p.4.

assessment or risk assessment methodology will be the second layer to fully responding to this recommendation.

In addition, the Italian SA “Garante”, has published an online self-assessment to help the data identify the actions to take following a personal data breach.²³ Although this is not strictly speaking a risk assessment methodology for data breaches, it is a useful practical tool for Italian organisations when taking decisions post-data breach incidents. However, the same issue as the ‘Evaluate-Risk GDPR tool’ by the AEPD is presented; the fact that only Italian organisations can rely on this since it is in Italian and considers the specific Italian data protection laws. Once again, **the recommendation of allocating specific areas for tool development to SAs is appealing, or at least ensuring that such tools will be available to all other European member states as well.** Nonetheless, this tool still does not cover the gap previously identified.

Finally, the AEPD published a Guide on personal data breach management and notification, which is the closest to the recommendation D3.4 provided. On the one hand, it provides a more complete methodology of ‘preparation, detection, identification, and classification’.²⁴ The Guide provides some insight into how to detect, identify, and manage data breaches, however it is a more descriptive Guide than providing a sound risk assessment method for data breaches. Essentially, it collates the different factors that must be considered, which is a useful first step. The AEPD has also provided a tool to notify the data breaches.²⁵

In conclusion, progress has been made with regards to how organisations should manage and react to data breaches. However, these guides are complementary to one another, making the process of preparation, managing and mitigation even more burdensome for organisations that may not have unlimited resources. In addition, a **complete and update on the assessment of the severity of breaches – by using the risk-based approach – is yet to be provided.**

2.1.2 Remaining challenges

2.1.2.1 Transfers to non-EU countries

The Court of Justice of the EU’s (CJEU) judgment in in Case C-311/18 (Schrems II) on July 2020 shifted the rhetoric for data transfers in the EU.²⁶ On the one hand, the adequacy decision for transfers from the European Economic Area (EEA) to the US, namely the “EU-U.S. Privacy Shield” got invalidated as a transfer mechanism. On the other hand, the Standard Contractual Clauses (SCCs), the most common transfer mechanism, remained valid. However, the CJEU highlighted that the validity of the SCCs is dependent on the data exporter’s (the organisation that transfers the personal data from the EEA to a third country) assessment on the “circumstances of the transfer”, meaning that it shall be assessed that the receiving country guarantees a level of protection “essentially equivalent” to that guaranteed within the EU.²⁷ The first

²³ Autovalutazione per individuare le azioni da intraprendere a seguito di una violazione dei dati personali, Garante, <https://servizi.gdpd.it/databreach/s/self-assessment>.

²⁴ Guide on personal data breach management and notification, AEPD, available at: <https://www.aepd.es/sites/default/files/2019-09/Guide-on-personal-data-breach.pdf>.

²⁵ The tool can be found here: <https://www.aepd.es/en/guides-and-tools/tools/comunica-brecha-rgpd>.

²⁶ 2020 Annual Report Ensuring Data Protection Rights in a Changing World 2020, European Data Protection Board

²⁷ Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems, European Data Protection Board, 23 July 2020, FAQ nr. 1, Available at: https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjec31118_en.pdf.

layer of complexity is introduced by the increased amount of research, reflections and aspects that a company needs to consider in order to properly carry out such an assessment. The Court but also the EDPB's Recommendations on the supplementary measures have included a list of non-exhaustive factors that must be considered in order for a company to have a valid personal data transfer from the EEA to the U.S. or other third countries.²⁸ This assessment must take into consideration, for example, all actors participating in the transfer (controllers, processors, sub-processors processing data in the third country), any onward transfers that may occur, the domestic legal order of the country to which the data is transferred (or onward transferred) but also the domestic practices.²⁹ Essentially, exporters must assess any factor that could potentially impact the effectiveness of the SCCs agreed between the parties.

The second layer of complexity and uncertainty is presented by the subjective results of the aforementioned assessment. If the assessment reveals that the effectiveness of the transfer mechanism is hindered due to the specific circumstances of the third country which the personal data is being transferred, organisations have to consider additional "supplementary measures" in order to ensure an essentially equivalent level of protection.³⁰ The nature of the supplementary measures may be contractual, technical, organisational or a combination, and they need to be identified on a case-by-case basis. The EDPB's list of non-exhaustive technical, contractual and organisational measures in Annex 2 of its Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data are a first practical approach to legal compliance for data exporters. However, the EU data exporters have a challenging task at hand, creating methodologies for carrying out such assessments internally within their organisation, implementing them, and updating them when necessary.

Although initially the Schrems II decision had the scope of checking the validity of the E.U-U.S. Privacy Shield, and therefore only influencing the transfers from the EU to the U.S., the decision ended up impacting all data flows outside the EU. It is unquestionable that the Schrems II decision provided higher legal certainty and level of protection in the transfers of data from the EU to third countries, however, this came at a cost of complex assessments challenging implementation of supplementary measures for transfers. It is reasonable that this challenge is especially felt by SMEs and start-ups, which do not have many resources to deploy for the purpose of legal compliance.

The demand for more guidance, advice and practical tools to implement the latest advancements on non-EU transfers of data was also demonstrated in the webinar carried out in collaboration with Digital SME on the "Schrems II Decision" on 30th of June 2021.³¹ Based on the results (see Annex C for a summary of the results) of the GDPR Temperature Tool 48% of companies that completed the tool carry out transfers outside the EU, while 53% of the companies had an annual worldwide turnover of up to 500.000 euro. This means that further guidance on data transfers is needed also among SMEs, since it almost half of the companies we surveyed transferred data outside the EU (see Annex C for a summary of the results). During the Schrems II workshop, the feedback we received was clear, namely that SMEs need to understand

²⁸ Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0, Adopted on 18 June 2020, European Data Protection Board, page 9, available at: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

²⁹ *ibid*, page 12.

³⁰ C-311/18 (Schrems II), paragraphs 130 and 133.

³¹ Information about the webinar event is available at: <https://www.cyberwatching.eu/news-events/events/schrems-ii-data-transfers-decision-impact-smes>.

whether they are transferring data, and if they do, it is a challenge to leverage their service providers in order to assess whether their data processing is compliant with the EU legislation and recommendations of the EDPB. This often seems to be connected to the negotiating power of SMEs as opposed to multinational companies.

Another more recent update which will also require further guidance in implementation and adequate time to properly comply with is the new set of Standard Contractual Clauses published on 4th June 2021, and that entered into force twenty days after the publication in the Official Journal of the European Union (27th June 2021). The old version of the Standard Contractual Clauses which have been relied on by companies until 2021 will be **repealed three months after the new SCCs enter into force** (27th September 2021). This means that if, after that date, a company enters into new contracts with non-EU processors after the old SCCs were repealed, the new SCCs must be used. Alternatively, if the company concluded a contract including the old SCCs prior to the date of their repeal, it will **remain a valid transfer mechanism for 15 months following the date of their repeal (until 27th December 2022)**. In short, the European Commission has approximately given a transition period of 18 months, for companies to both embed the new SCCs into their future data protection relationships as well as substitute the old SCCs with the new version. Other than a transitional time, the new SCCs will require guidance in terms of the supplementary measures that must be entered into, as well as tools that can ease the assessment that must be carried out by companies. As a matter of fact, the new SCCs perfectly embed the requirements set forth in the Schrems II decision and in the EDPB recommendations, since they do not act in a vacuum but still require the data exporter to carry out a data transfer impact assessment and evaluate the necessity of supplementary measures.³² An important recommendation that arises on this topic is the **necessity for a data transfer impact assessment, which will assist organisations to assess all relevant factors and considerations before carrying out data transfers outside the EEA.**

In conclusion, although legal certainty has increased with the updated rules on data transfers, the complexity of the environment is a challenge that all SMEs, start-ups and European research projects must overcome. The policy makers and enforcement authorities, like data protection authorities, must ensure that adequate support is provided to the cyberwatching.eu stakeholders to this regard.

2.1.2.2 Risk Assessments and Data Protection Impact Assessments

According to our survey on the GDPR compliance posture of SMEs (see Annex C for the results of the survey), 40% of the companies have not carried out a risk assessment for the processing activities that they conduct; nor subsequently implemented appropriate technical and organisational measures to ensure and be able to demonstrate that they process personal data in accordance with GDPR. In addition, 43% have not identified the processing activities subject to a Data Protection Impact Assessment. From those that have identified the need for a DPIA only 62% of the companies have already conducted it. These results, but also based on the partners' experience, the risk assessments and DPIAs remain a challenge for many companies – whether it be SMEs or multinational companies.

As mentioned also in D3.4, the subjectivity of the risk-based approach opens up grey areas for entities which process personal data (such as SMEs). Therefore, the recommendation of cyberwatching.eu for both research projects and policy makers is to **create a “framework”, which can be utilised by controllers with the aim of guiding them in assessing the risks of their processing operations in a complete**

³² See clause 14 of the updated Standard Contractual Clauses.

manner. This “framework” can produce several objective factors or indicators that may guide, in a non-inclusive way, the determination of the risk assessment. In order for policy-makers to be able to create such a structure, the realistic outlook of each industry must be taken into account, meaning that an open discussion can stir the structure of risk assessments in a way that will not only include the theoretical aspects but also present them in a practical and manageable manner.

Therefore, we re-iterate the recommendation initially raised in the previous deliverable D3.4 (Cybersecurity, legal and policy aspects, preliminary recommendations, and road ahead) it is necessary to publish “a systematic methodology for GDPR risk assessments”, which will facilitate the implementation of the risk-based approach in a practical manner but also ensure consistency between the risk assessments carried out by companies. Furthermore, another useful recommendation to address this challenge, which was also preliminary posed in deliverable 3, could be the **creation of a European tool for Data Protection Impact Assessments which could compile the several applicable national black lists**. In order to get as concrete as possible, a tool that could help initiate such a pan-european instrument is the tool already created by the French Supervisory Authority carrying out data protection impact assessment.³³ This existing tool could be used by policy makers and EU Projects as starting point to get an updated and pan-european version.

2.1.2.3 Data Breach Management

The statistics we collected on the area of data breach management were concerning. According to our survey on the GDPR compliance posture, only half (52%) of the respondents have developed a personal data breach management procedure. The availability of a data breach management process or procedure is an ancillary obligation, nonetheless, it remains an important aspect of the efforts to safeguard and respect the data subjects’ rights and freedoms. This obligation arises from article 33 and 34 of the GDPR, whereby a notification must be communicated to the supervisory authority within 72 hours, and under certain circumstances, the individuals whose personal data were affected by the breach. Further, the GDPR requires the controller to document any personal data breaches by collecting the facts relating to it, its effects and any actions taken to remediate those effects.³⁴ Although the GDPR does not explicitly mention that a data breach management procedure must be present, based on the Consortium’s experience in the application of the GDPR and the two sub-requirements in relation to data breaches, having a data breach management procedure is a necessary component for organisations for both documentation purposes as well as rapidly and efficient responses to data breach incidents.

In addition, based on the latest Guidelines on examples regarding Data Breach Notification by the European Data Protection Board, it became clear that “a need has arisen for a practice-oriented, case-based guidance” that also shares the experience gained by Supervisory Authorities in the GDPR application.³⁵ The Guidelines point out that “every controller should have plans, procedures in place for handling eventual data breaches” and that there must be clear internal reporting processes and persons’ responsibilities for assisting the recovery process.³⁶ Further, the European Union’s Cybersecurity Agency (ENISA) has also listed the development of an incident

³³ The French Privacy Impact Assessment (PIA) is available at <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment>.

³⁴ Article 33 (5) General Data Protection Regulation.

³⁵ Guidelines 01/2021 on Examples regarding Data Breach Notification, Adopted on 14 January 2021, Version 1.0, p.4.

³⁶ Guidelines 01/2021 on Examples regarding Data Breach Notification, Adopted on 14 January 2021, Version 1.0, p.6.

response plan as a prerequisite to “respond[ing] quickly to security threats”.³⁷ Specifically, ENISA suggests for SMEs to investigate tools for monitoring and alerting the organisation when suspicious activity or security breaches occur.

As a result of the above, and of the analysis of the responses collected from the GDPR Temperature tool, it is clear that the level of preparedness of SMEs is not sufficient. A lack of a data breach management procedure can be interpreted as signal for a general lack of awareness, preparation and role definition. Therefore, a more in-depth level of explanation on the aspects of compliance in relation to data breaches, such as implementing a data breach management procedure, investigating tools and security measures to mitigate the effect of data breaches is necessary.

As mentioned above, the GDPR Temperature tool created by cyberwatching.eu has been updated with its 2.0 version. This version already aims to assist the above gaps and challenges posed to SMEs with regards to this area. Firstly, the tool's recommendations list a minimum set of considerations that must be embedded in the process of evaluating the likelihood that the breach results in risks to the rights and freedoms of the data subjects by applying. By relying on the Recommendations for a methodology of the assessment of severity of personal data breaches published by ENISA, the SMEs can be handed with a more straightforward and short explanation of the essence of a ‘personal data breach severity assessment’.³⁸ The implementation of this assessment in their data breach management procedure can ensure a consistent and efficient process when the SME decides whether the supervisory authority and the data subjects must be notified.

2.1.2.4 Clarifications on the intricacies between GDPR and NIS

The preliminary recommendation on the necessary clarifications on the intricacies between GDPR and NIS remains, as no progress has been made to this regard. In the Second Concertation Meeting all stakeholders mentioned the need for guidance on sanctions for violations and time efficient compliant procedures in each industry. For example, the industry could shed light on the procedures that take place in real time when security incidents occur within Operators of Essential Services (OES) and **further research can help find the most time-efficient and compliant method of managing notifications that fulfill the requirements of both the NISD and the GDPR.** In addition, policy-makers could provide guidance for organisations on the extent to which sanctions will be applied for both legislations and how such violations will be regarded by competent authorities and member states.

2.2 Compliance of Emerging Technologies

As it has been introduced in the preliminary recommendations of D3.4 and enhanced in D3.5 on Risk and recommendations on cybersecurity services, the compliance of emerging technologies, such as AI and IoT, come with the theoretical and practical challenge of implementing the general GDPR and NISD principles in more innovative, specific, and intrusive digital environments. Many of the Cyberwatching.eu services involve emerging technologies, and therefore this White Paper will also assess the progress made with regards to the challenges posed to emerging technologies and identify the challenges that remain to be addressed in these sectors. Although blockchain has also been analysed previously, it seems to be less relevant and prevalent among SMEs and projects of Cyberwatching.eu, thus is it the reason why this White Paper did not go into detail on it.

³⁷ Cybersecurity guide for SMEs - 12 steps to securing your business, European Union Agency for Cybersecurity, p. 5, available here: <https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes>.

³⁸ Recommendations for a methodology of the assessment of severity of personal data breaches, p. 9.

On the one hand, some challenges include a lack of understanding of whether the GDPR obligations are at all relevant to developers/providers and users of Emerging Technologies. On the other hand, it is also challenging to decide how to adapt the obligations in order for them to remain relevant, and not be conflicting with the very essence of the Emerging Technologies. In contrast, the main concerns related to the NISD lie in the implications around injecting Emerging Technologies into the operations of the Operators of Essential Services (OESs) and Digital Service Providers (DSPs), and to what extent this can be done without sacrificing security, usability and traceability of networks and information systems.

Further, technology service developers/providers – which, frequently, can be classified as micro, small or medium enterprises (SMEs), in light of their reduced number of employees and annual turnover³⁹ – are consistently giving light to new and innovative ideas to improve service or products, notably by connecting them to the Internet or by designing/adapting them around the use of artificial intelligence (“AI”) models.

These types of emerging technologies present specific and significant challenges, both in terms of legal compliance and in terms of adherence to ethical and transparency-related principles. The European Union, including by way of initiatives seeking to promote the making of AI software and hardware more “*human-centric*”,⁴⁰ has demonstrated its commitment to mitigating the perceived risks to the fundamental rights, freedoms and legitimate interests of individuals which may arise from the use of AI. In particular, where such systems involve the use of personal data, the fundamental rights to privacy and protection of personal data – enshrined in Arts. 7 and 8 of the Charter of Fundamental Rights of the European Union⁴¹ – are inherently affected, and all the more so where massive amounts of personal data are collected by such systems, in manners potentially unknown or unclear to the data subjects concerned. This applies also to systems built around ‘Internet of Things’ functionalities (IoT), which allow the connection of everyday objects – such as cell phones, wearable devices, cars, washing machines and refrigerators – to the Internet, so that they can exchange information between each other;⁴² in particular, because such systems rely on the processing of data (including personal data) to such an extent that the concept of IoT has previously been linked, by the Article 29 Data Protection Working Party,⁴³ to the notions of ‘pervasive’ and ‘ubiquitous’ computing, thereby “*clearly [raising] new and significant personal data protection and privacy challenges*”.⁴⁴ As such, with an aim to avoid causing undue harm to the data subjects concerned, any such processing of personal data must comply with the GDPR’s principles relating to the processing of personal data⁴⁵; in particular, any foreseen activities involving the processing of

³⁹ See Annex to Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, Art. 2, available at:

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361>.

⁴⁰ European Parliamentary Research Service, *EU guidelines on ethics in artificial intelligence: Context and implementation*, (September 2019), p. 3, available at:

[https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI\(2019\)640163_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf)

⁴¹ Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>.

⁴² European Data Protection Supervisor, *Internet of Things*, available at: https://edps.europa.eu/data-protection/our-work/subjects/internet-things_en.

⁴³ The Article 29 Data Protection Working Party was an independent European working party that dealt with issues relating to the protection of privacy and Personal Data until 25 May 2018 (entry into application of the GDPR), at which point it was replaced by the European Data Protection Board.

⁴⁴ Article 29 Data Protection Working Party, *Opinion 8/2014 on the on Recent Developments on the Internet of Things* (16 September 2014), p. 4, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

⁴⁵ Established in Art. 5 GDPR: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, security (integrity and confidentiality) and accountability.

personal data, including by use of these emerging technologies, must be subjected to strict assessments as to their necessity⁴⁶ and proportionality⁴⁷.

It is worth noting that the proposal Regulation published in April 2021 laying down harmonised rule of Artificial Intelligence (Artificial Intelligence Act) will be a crucial component of further advancing, clarifying, and solidifying the obligations with regards to Artificial Intelligence. Nonetheless such progress has not been made in IoT, and thus most of the challenges preliminary posed remain in this sector.

On a more general note, stakeholders recommended that **for emerging technologies there must be practical tools (possibly open source) that are specifically focused on compliance of emerging technologies and that are kept up to date according to the industry standards and state of art as well as rate of change of the technologies.** While, this is undoubtedly a challenging recommendation, cyberwatching.eu believes it could be concretely achievable by **combining the precious expertise of ENISA with the core projects that have been launched and that will be launched in the context of Horizon Europe.** The alliance of those players could allow for practical tools that are updated on a semester or yearly basis, according to the industry changes and state of art. For this final objective to be achieved it is believed that the **interaction with the industry sector will be crucial**; for this reason, this recommendation can be considered as also referred to DEP. This interaction could also be linked to roadmapping exercises that aim to identify which technologies are likely to be adopted.

In addition, it has been frequently mentioned that there must be a continuous “loop of mutual feedbacks” between the policy makers, the research and the market or industry. This recommendation suggests that in the medium-term, the **DEP should aim at drafting a structured flow of information that facilitates the continuous sharing of feedback between policy makers, research initiative and industry on matters regarding emerging technologies.** This recommendation ties perfectly with the aforementioned suggestion for Horizon Europe (*Open source tools for compliance of emerging technologies that are periodically updated according to the state of art*) and give the DEP the mandate of coordinating the industry in order to find an appropriate method for an advantageous and continuous sharing of information. Once this method is decided, then all stakeholders can be part of a larger conversation that would include:

- the industry players, who innovate their products and services and enhance emerging technologies,
- researchers, who help find the gaps of those technologies and recommend methods to close those gaps,
- trainers, who combine the information in order to give back to the community,
- and policy-makers, who can use that feedback constructively in their next legislative initiatives or soft-law guidance.

⁴⁶ See, e.g., European Data Protection Supervisor, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, (11 April 2017), available at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf.

⁴⁷ As noted by the European Data Protection Supervisor, the “*Processing of personal data - be it collection, storage, use or disclosure - constitutes a limitation on the right to the protection of personal data and must comply with EU law.*” More information on this can be found in the *EDPS quick-guide to necessity and proportionality*, (n.d.), available at: https://edps.europa.eu/sites/edp/files/publication/20-01-28_edps_quickguide_en.pdf

2.3 Artificial Intelligence (AI)

Artificial intelligence (AI) is increasingly becoming an integral part of technology and cyberspace. AI can be implemented in systems, software and devices of varying sectors, to similar degrees of effectiveness.⁴⁸ From the data protection perspective, AI is typically used as a tool for automated decision-making and profiling, by leveraging algorithms to process large volumes of data.⁴⁹ In terms of AI being implemented in critical infrastructures, countries are putting AI to use in order to offer better and faster telecommunication services to citizens, run trade and stock markets by algorithms, or even create governmental procedures for voting, and managing administrative complaints.⁵⁰ In this context, the main challenges arise when the processing activities carried out by means of AI are capable of leading to automated decisions which produce legal, or similarly significant effects on data subjects.⁵¹

2.3.1 Progress made

2.3.1.1 Ethics and Trustworthy AI

As mentioned in D3.7 a challenge that could not be overcome by the current regulations alone, was that of the relationship with transparency and ethics.⁵² Since the previous deliverable 3.4, substantial progress has been made to this regard. Firstly, the *Ethics guidelines for trustworthy AI* were published to aid the development of trustworthy AI in the European context.⁵³ The High-Level Expert Group (“HLEG”) through Artificial Intelligence’s ‘Trustworthy AI’ pointed out that AI should be lawful, ethical, and robust.⁵⁴ In addition, the practical list to self-assess the trustworthiness of AI in July 2020 has also attempted to support and revise the guidelines.⁵⁵

The HLEG Guidelines provide with a useful framework, based on seven requirements for artificial intelligence in order for it to be considered to be trustworthy.⁵⁶ Trustworthiness can be seen as a necessary prerequisite for the ultimate success of the Emerging Technologies as, in absence of trust, the Emerging Technologies may not see widespread use. These requirements include (1) the involvement of human agency and oversight, calling for AI to empower individuals and promote their fundamental rights; (2) technical robustness and safety, ensuring that AI is both secure and resilient; (3) privacy and data governance, guaranteeing compliance with law and

⁴⁸ For more on this, see Consultative Committee of the Convention of the Protection of Individuals with regard to Automatic Processing of Personal Data, *Guidelines on Artificial Intelligence and Data Protection* (25 January 2019), available at: <https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8>.

⁴⁹ For more on this, see UK Information Commissioner’s Office, *Big data, artificial intelligence, machine learning and data protection* (4 September 2017), available at:

<https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>.

⁵⁰ European Commission, *Statement on Artificial Intelligence, Robotics and ‘Autonomous’ Systems* (9 March 2018), available at: https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf.

⁵¹ See Art. 22(1) GDPR.

⁵² European Parliamentary Research Service, *EU guidelines on ethics in artificial intelligence: Context and implementation*, (September 2019), p. 3, available at:

[https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI\(2019\)640163_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf).

⁵³ High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for a trustworthy AI* (8 April 2019), available at: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.

⁵⁴ High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for a trustworthy AI* (8 April 2019), p. 5, available at: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.

⁵⁵ European Commission, *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*, 17 July 2020, available at: <https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>.

⁵⁶ High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for a trustworthy AI* (8 April 2019), pp. 14-20, available at: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.

also fostering acceptable data governance mechanisms; (4) transparency, with respect to the data used, the system itself and the actual business model of the AI; (5) diversity, non-discrimination and fairness, circumventing bias and promoting diversity; (6) societal and environmental well-being which calls for AI to positively contribute to society; and finally, (7) accountability, which calls for the implementation of mechanisms that ensure AI systems are accountable and responsible.

On a positive note, we can report that the previous recommendation of D3.4 to create user-friendly instruments to disseminate Ethics guidelines for AI has been taken into account by policy makers and specifically by the AI HLEG. Specifically, the stakeholders had mentioned that the [Ethics guidelines for trustworthy AI](#) presented in April 2019 by the European Commission's High-Level Expert Group on AI cannot be considered easily comprehensible and concretely usable by all the organisations deploying AI. On 17 July 2020, AI HLEG published "The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment"⁵⁷, which is a tool that supports the above "[Ethics Guidelines for Trustworthy Artificial Intelligence](#)" (AI) and the seven key requirements of trustworthy AI. This web-based tool is in the form of an accessible and dynamic checklist, which allows for businesses and organisations, developers and deployers of AI to self-assess their systems under development through concrete steps, as well as to ensure that their users can benefit from AI without being exposed to unnecessary risks.⁵⁸

2.3.1.2 Risk Analysis and Risk Assessment for AI

The risk assessment approach has been consistently a challenge for all SMEs due to the number of factors that must be considered, and the lack of methodology provided, as also pointed out in sections 2.1.1. and 2.1.2.2. However, the risk assessment related to AI poses an even greater challenge due to the evolving factors of the processing activities. Specifically, the circumstances that the risk of the processing and, at times, the envisaged consequences for data subjects may not be comprehensively analysed beforehand by the controller. The same argument has been outlined in several deliverables of cyberwatching.eu before, including the D3.4, and D3.5.

The preliminary recommendation suggested in D3.4 was to **create guidelines on methodology for risk analysis, specifically related to AI which would take the evolving aspects of AI into consideration**. However, this challenge has not yet been fully overcome. Although progress has been made to this regard through the introduction of the Artificial Intelligence Act (AIA), which only provides a solid risk methodology to define "high risk" AI systems that pose significant risks to the health and safety or fundamental rights of persons, taking into account both the severity of the possible harm and its probability of occurrence.⁵⁹ Recital 32 of the AIA further specifies that the classification of high-risk AI should be considered in light of the specific AI systems' intended purpose. It is also useful that AI systems have been categorised into minimal risk, limited risk, high-risk and unacceptable risk.

⁵⁷ *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment* available at <https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>

⁵⁸ Web-based self-assessment AI tool available at <https://futurium.ec.europa.eu/en/european-ai-alliance/pages/altai-assessment-list-trustworthy-artificial-intelligence>

⁵⁹ Proposal for A Regulation of The European Parliament and of The Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts COM/2021/206 Final, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>.

The above criteria to determine a “high risk” AI system is further supported through a list of specific sectors whereby the implementation of AI technology would be considered “high risk”, namely, critical infrastructures such as transport (the health of citizens is at risk), educational or vocational training (the risk of access to education and progress in professional career), safety components of products (AI application in robot-assisted surgery), employment (decision making carried out through recruitment software implementing AI), essential private and public services (credit scoring risking economic opportunities for citizens), law enforcement (impact to people’s fundamental rights), migration (risk to discrimination or verification of authenticity of travel documents), administration of justice and democratic processes.⁶⁰

However, the aspect of the risk-based approach has not yet been formed into a practical methodology of analysing, identifying, and deciding whether a system of AI is of high-risk or not. The AIA proposal to some extent overcomes the challenge that AI systems’ developers and providers had prior to the proposal, whereby they were called to rely on the risk-based approach introduced by the GDPR. However, there is still room for enhancing the provided framework of the AIA proposal, which now includes a wide definition of some types of high-risk systems. **Therefore, it is recommended for policy makers to ensure the inclusion of a methodology for risk analysis relating to all levels of risk of AI, which should aim at further clarifying the ever-changing aspects of AI.** This amendment will ensure both consistency of methodology between determining low-risk and high-risk AI systems, but will also ensure that the level of risk is duly increased when the application of the AI system is changed or adapted.

The EU could gain inspiration from other such risk assessments around the world, for example from the Canadian Algorithmic Impact Assessment (AIA).⁶¹ The AIA was designed in order to assess and manage risks related to automated decision-making, and was borne from the Canadian Directive on Automated Decision-making, aiming to “ensure that Automated Decision Systems are deployed in a manner that reduces risks to Canadians and federal institutions, and leads to more efficient, accurate, consistent, and interpretable decisions made pursuant to Canadian law”.⁶² In this way, the Canadian Government has demonstrated its commitment to the principles of “transparency, accountability, legality, and procedural fairness”,⁶³ principles which are also enshrined in European legislation.

Further, another kind of risk assessment that could be developed and carried out by market operators is the already-used fundamental rights impact assessment of the Charter of Fundamental Rights of the European Union’s implementation.⁶⁴ It provides an assessment method that allows for the analysis of the influence a specific policy

⁶⁰ Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence, Press Release, 21 April 2021, Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682.

⁶¹ Government of Canada, *Algorithmic Impact Assessment (AIA)*, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>.

<https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/responsible-use-ai/algorithmic-impact-assessment.html>.

⁶² The Government of Canada implemented the Directive on Automated Decision-Making, which took effect on 1 April 2019 and of which compliance is mandatory from 1 April 2020. The Directive can be accessed here: <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592>.

⁶³ Government of Canada, *Directive on Automated Decision-Making* (1 April 2019), available at: <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592>.

⁶⁴ See also European Commission, *Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union* (19 October 2010), available at: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52010DC0573>.

may have on the fundamental rights of EU citizens, thereby seeking to ensure the compliance of that policy with the Charter.⁶⁵ The development of a risk assessment framework for industry that is based on the EU's fundamental rights risk assessment, taking into consideration the real and potential risks to the rights and freedoms of individuals that are implicated in AI systems, could help mitigate such risks and ensure the development of transparent and ethical Emerging Technologies.

The EDPS has also issued relevant Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data⁶⁶ and a toolkit,⁶⁷ from which inspiration could also be taken for the development of an AI risk assessment (as well as the ALTAI tool as described in Section 2.3.1.1) On the one hand, this assessment could evaluate necessity, through the identification of the fundamental rights and freedoms potentially impacted, the system's objectives and the relevant interests behind it to ensure that the system is the least intrusive in order to avoid negatively affecting rights and freedoms. On the other hand, a proportionality assessment would act as a balancing test to ensure that the results of the system are aligned with its objectives. Lastly, this assessment would also evaluate that the data processing in terms of scope, extent and intrusiveness, and check that adequate safeguards are in place to improve proportionality if needed.⁶⁸

Furthermore, to be able to provide a concrete risk analysis and overcome this challenging goal, the Supervisory Authorities have an important role as well. As a matter of fact, while fulfilling their tasks, they contact many entities that process personal data, and this gives them the possibility to also get to know the state of art when it comes to sector-specific activities of processing. Furthermore, a recommendation that can be addressed to policy makers is to **consider broadening the tasks of Supervisory Authorities (Art. 57 GDPR), and evaluating the opportunity of finding an efficient instrument that allows entities that process personal data to ask for guidelines on the most challenging obligations they face, especially when it comes to emerging technologies.**

As a conclusion, although progress has been made with regards to risk analysis and risk assessment of AI by means of latest AIA proposal, there are still challenges to overcome in this area. Some of the recommendations suggested target the policy makers that now have the unique opportunity to further elaborate the AIA proposal with the most necessary components, such as the embedding of a risk assessment methodology. Other recommendations target the SAs and other relevant actors, such as the AI High-Level Expert Group that can create further guidelines, tools and practical instruments for the implementation of the risk-based approach in AI systems.

⁶⁵ European Commission, Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments (6 May 2011), p. 3, available at: https://ec.europa.eu/info/sites/info/files/operational-guidance-fundamental-rights-in-impact-assessments_en.pdf.

⁶⁶ European Data Protection Supervisor, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (19 December 2019), available at: https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.

⁶⁷ European Data Protection Supervisor, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, (11 April 2017), available at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf.

⁶⁸ This methodology is based on the European Data Protection Supervisor's *Quick-guide to necessity and proportionality*, available at: https://edps.europa.eu/sites/edp/files/publication/20-01-28_edps_q9quickguide_en.pdf.

2.3.2 Challenges remaining

2.3.2.1 Challenges of Data Minimisation

The challenge of data minimisation is at the heart of the data protection issues that arises from the use of AI. The GDPR principle goes against the purposes and functions of AI itself, which is for the AI's algorithm to generate accurate and useful results, or even further develop (in the case of machine-learning algorithms) by using large datasets. This is especially the case for more advanced machine learning (ML) algorithms, for example neural networks, which require large volumes of data to make predictions or classifications.⁶⁹ The paradox between AI and data minimisation is that even contextual data may be important for AI⁷⁰, since AI algorithms will rely on data that may not be strictly relevant for the specific purpose, to ensure that AI can also learn to identify and discard data which is irrelevant to that goal. These characteristics of AI algorithms have been developed to increase the algorithms' effectiveness after deployment.⁷¹

However, the challenge is that this very nature of AI goes against the traditional requirements for data minimisation which aim to only process personal data which is "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".⁷² Further, AI developers may not be capable of correctly predicting how much data (necessary or contextual) an AI algorithm will need in order to deliver the expected output, since this depends on different factors, such as the training speed or accuracy of a specific AI model.

It is pertinent to distinguish between data minimisation, on the one hand, during the training phase of the model algorithm (original training data), and, on the other hand, the inference phase, which is once the AI model is used to make predictions or classifications while running on new or real-time data.⁷³ Both phases would be needed to avoid inaccuracy, ensure fairness, and lack of discrimination in the AI decision-making. If the model is used for predictions or classifications about individual people, for example to decide whether a loan must be given to an individual, then it is most likely that personal data will be used both in the training and inference phases.⁷⁴

Furthermore, AI developers must consider, firstly, the complexity of the problem or processing that the AI model is targeting, and secondly the complexity of the learning algorithm, to evaluate the adequacy, necessity or relevance of a given dataset for AI-based processing activities. Firstly, bearing in mind the complexity of the processing

⁶⁹ Abigail Goldsteen et al., Data Minimization for GDPR Compliance in Machine Learning Models, Cornell University (2020), <https://arxiv.org/pdf/2008.04113.pdf>, p. 1.

⁷⁰ For simplicity's sake, consider the following example: if a developer is building an AI-based system to visually recognize fruit, the AI's training dataset may also need to include not only images of fruit, but also of any other objects or materials that may be mistaken for fruit, so that the AI learns what input to reject (and not just what input to accept).

⁷¹ For more information on this, see European Parliament, *Understanding algorithmic decision-making: Opportunities and challenges* (March 2019), available at: [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU\(2019\)624261_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf).

⁷² Art. 5(1)(c) GDPR.

⁷³ Information Commissioner's Office, *Guidance on AI and data protection, How Should We Assess Security and Data Minimisation in AI?*, available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection/how-should-we-assess-security-and-data-minimisation-in-ai/>.

⁷⁴ Information Commissioner's Office, *Guidance on AI and data protection, How Should We Assess Security and Data Minimisation in AI?*, available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection/how-should-we-assess-security-and-data-minimisation-in-ai/>.

in this two-fold way can help define the fundamental functions that the algorithm must achieve, which can also help identify what input data (categories and volumes of data) the algorithm will require. Secondly, deliberating the complexity of the learning algorithm can help to understand how the data analysis will occur through the algorithm, which may call for a more precise identification of the types of personal data that would be “adequate, relevant and necessary” for the AI model to meet its intended purpose.

The important take-away from this principle for AI systems’ developers is to only process the personal data they need for the specific purpose of the training and inference phases of the AI. It is important to note that there are different ways with which AI or machine learning developers and architects can **create privacy-preserving techniques in compliance with data minimisation into both the training and the inference phase of the AI system.**⁷⁵ Valuable techniques for minimising the personal data being processed during the training phase are the addition of ‘noise’ to the data, which consists of the random altering of certain values of data points belonging to individuals⁷⁶, or the use of synthetic data, which is data that has been generated artificially.⁷⁷ When it comes to the inference stage, a common privacy preserving technique is to reduce the ‘personality’ of the available data, rather than the amount of the data – for example, through technical measures that would pseudonymise the personal data.⁷⁸ Another technique is to convert the personal data into less ‘human readable’ formats, which would transform raw personal data into an abstract format for the purposes of prediction or classification.⁷⁹ In addition, inferences can be made locally, for example, the AI model may be installed on the user’s local device instead of it being hosted on a cloud server.⁸⁰

In addition, three considerations may be given in reducing the challenge between the use of large volumes of data and the principle of data minimisation. Firstly, **the principle of proportionality should be linked to the principle of minimisation.** Specifically, when additional personal data must be processed for the purpose of training, increases the accuracy, or reducing the discrimination of the AI model, there should be a proportionality assessment. To carry out this assessment the AI developer should evaluate whether this additional personal data provides a benefit, in relation to the purposes of the processing, which outweighs the risks posed to the data subjects.

⁷⁵ Better Machine Learning Through Data Minimization, Privatar (March 5, 2020), <https://www.privatar.com/blog/better-machine-learning-through-data-minimization>.

⁷⁶ An AI system developer could choose the level of noise injection depending on the circumstances and the purposes of the AI system. There are limitations to this privacy preserving technique which is the risk for less accuracy at an individual level. However, if the AI system has enough individuals’ data points, a general pattern may still be observed and be sufficient for the purpose of training the AI model at a first phase.

⁷⁷ The Information Commissioner’s Office, Guidance on AI and data protection, How should we assess security and data minimisation in AI?, Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection/how-should-we-assess-security-and-data-minimisation-in-ai/>.

⁷⁸ European Parliamentary Research Service, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, available at: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf), p. 90.

⁷⁹ The Information Commissioner’s Office, Guidance on AI and data protection, How should we assess security and data minimisation in AI?, Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection/how-should-we-assess-security-and-data-minimisation-in-ai/>.

⁸⁰ *Ibid.*

⁸¹ Secondly, should the personal data be processed merely for statistical purposes for example as training data input, the principle of data minimisation can be interpreted in a less strict manner.⁸² It is recommended that the **AI developer should be able to distinguish the compliance with the principle of data minimisation between the cases of statistical processing for the objective of producing statistical surveys or results, and the ones where the personal data are used for predictions, or decisions that can affect individuals.**⁸³

In conclusion, all stakeholders participating to the round-table discussions in the Concertation Meetings observed that this presumed need to process big data should be balanced with the obligation to respect the principle of data minimisation. Furthermore, stakeholders observed that there is a lack of solid and technical guidance on this topic. In order to tackle this concern, it would be **recommended that further research be carried out on how the concept of data minimisation can be balanced against the inevitable necessity for mass data collection, in order to train algorithms within AI models and deploy AI and machine learning models.**

2.3.2.2 Challenges of Purpose Limitation

According to the GDPR's principle of purpose limitation,⁸⁴ personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes".⁸⁵ The Article 29 Data Protection Working Party ("WP29") has also noted that any processing that occurs after the collection of personal data, regardless of whether this purpose was initially disclosed or if it is an additional one, the processing must be classified as 'further processing'.⁸⁶ The practical importance of this classification is that if a further processing activity occurs, the requirement of compatibility must be met.⁸⁷ This notion of 'compatibility' is further explained in Art. 6(4) GDPR, which lays down the criteria to be assessed by a controller in order to establish if a further processing purpose is compatible with the initial purpose for data collection.⁸⁸ This compatibility assessment does not fully

⁸¹ European Parliamentary Research Service, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, available at: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf), p. 61.

⁸² *Ibid.*

⁸³ Recital 132 of General Data Protection Regulation.

⁸⁴ Art. 5(1)(b) GDPR.

⁸⁵ On this point, see Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation* (2 April 2013), available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, p. 15: "Personal data must be collected for specified purposes. The controller must therefore carefully consider what purpose or purposes the personal data will be used for, and must not collect personal data which are not necessary, adequate or relevant for the purpose or purposes which are intended to be served".

⁸⁶ Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation* (2 April 2013), p. 21, available at:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

⁸⁷ Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation* (2 April 2013), p. 21, available at:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

⁸⁸ Note that Art. 6(4) GDPR generally allows further processing to take place, even in the absence of compatibility with the original processing purposes, where consent is relied on as a legal basis for the further processing, or where the further processing is authorised by Union or Member State law. The compatibility assessment must consider five components: firstly, whether there is any link between these purposes; secondly the context in which the personal data was collected; thirdly, the nature of the personal data in question; fourthly, the possible consequences of the intended further processing for data subjects; and lastly, the existence of appropriate safeguards, such as encryption or pseudonymisation.

answer the common problem that arises in cases of reuse of repurposing of personal data in AI applications.⁸⁹

A frequent problem with machine-learning algorithms is the possibility for such algorithms to, autonomously (and in unexpected or unpredictable ways) process personal data for purposes different, or incompatible with, the original purposes for which the algorithms were set up. Machine-learning-based algorithms cannot only learn to achieve the goals they are programmed for but they can also reinterpret their goals, shifting the focus from achieving their original goals to achieving the feedback they would receive if they had done so.⁹⁰ Where this occurs the result is that personal data is processed for a purpose not originally disclosed to data subjects (i.e., not specified or explicit), and which may potentially be incompatible with the purposes for which personal data was originally collected. Such a result would inevitably collide with the principle of purpose limitation.

The Information Commissioner's Office (ICO) has published valuable guidance on the topic of purpose limitation by bringing forward the notion of separating the research and development phase of AI systems from the deployment phase due to them being different purposes, but also involving different circumstances and risks.⁹¹ The research phase would include the conceptualisation, design, training, and model section, while the deployment phase would consist of the actual implementation of the AI system in a real-world scenario. ICO specifies that an AI system may be developed for a general-purpose task, but it can be deployed in different contexts for different purposes. Further, it is clarified that if the AI system is implemented by a third party, the purpose of the processing for developing the AI system shall be different from the purpose of using the AI system (by the third party).

As can be concluded from the short guidance provided by the ICO, controllers should carefully analyse the systems that they wish to implement and ensure that they are able to provide clear and adequate information to data subjects on how those systems will work and, in particular, the purposes for which they will use personal data. Although ICO's guidance is a useful direction for how the principle of purpose limitation must be addressed by AI systems, there is still a need for more **guidelines or templates on how to disclose such information in a digestible way for individuals (consumers), considering, where relevant, the requirements of Art. 13(2)(f) and 14(2)(g) GDPR,**⁹² **could be of great benefit to AI developers and users.**

Nevertheless, the overall concern on the clash between purpose limitation and AI training and deployment can seemingly only be addressed by **imposing limitations or further requirements on the use of personal data within AI-based systems.** Algorithms (and machine-learning algorithms) should be carefully developed so that they will not, autonomously or beyond the control of the relevant controller, process personal data collected for purposes beyond the scope of their collection (or, at least, not without a proper compatibility test, under Art. 6(4) GDPR, having been performed by the relevant controller). Having that said, considering the fact that the European

⁸⁹ European Parliamentary Research Service, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, available at: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf), p. 46.

⁹⁰ For more on this, see, e.g., Casey Chu et al, CycleGAN, a Master of Steganography, available at: <https://arxiv.org/pdf/1712.02950.pdf>.

⁹¹ The Information Commissioner's Office, Guidance on AI and data protection, What do we need to do to ensure lawfulness, fairness, and transparency in AI systems?, Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection/what-do-we-need-to-do-to-ensure-lawfulness-fairness-and-transparency-in-ai-systems/>.

⁹² See Section 3.1.3, below.

Commission has proposed the Artificial Intelligence Act, this concern can either be overcome if either a) policy makers clarify, through the AIA, the tensions between the GDPR principle of purpose limitation and the training and deployment of AI systems, or should this not be feasible, if b) competent authorities provide guidance on the methodology that SMEs / start-ups training or implementing AI systems in their processes should follow.

2.3.2.3 Challenges of Transparency and Lawfulness

According to the GDPR's principle of transparency,⁹³ controllers are required to provide data subjects with information as to their activities involving the processing of personal data, under, e.g., Arts. 13 and 14 GDPR. Where automated decision-making occurs, the information provided must also include the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.⁹⁴ This approach aims to guarantee that data subjects understand exactly how their personal data will be used and what the consequences may be for them.

When AI-based systems are used to process personal data, difficulties arise in the provision of clear information to data subjects, not only because such systems are often very complex (thus hard to explain in a concise and intelligible manner to data subjects, as required by Art. 12(1) GDPR), but also because the purposes for which such systems may handle personal data may evolve over time.⁹⁵

According to the High-Level Expert Group on Artificial Intelligence, the requirement of transparency in AI “*is closely linked with the principle of explicability*” and it encompasses different transparency elements relevant to the AI system including the data, the system, and the business models.⁹⁶ In addition, the Ethics Guidelines for Trustworthy Artificial Intelligence have also established that traceability, explainability and communication play fundamental roles in transparency.

Traceability is important both with regards to the datasets used and the algorithms involved. It calls for the datasets that contribute to the AI's decision-making to be traceable, and for the algorithms used by the AI system to be adequately documented. As a result, it is highly suggested for AI system developers and architects to establish procedures and methods that concretely ensure traceability.⁹⁷ These procedures should guarantee that all possible outcomes of the decisions made by the AI are known

⁹³ Art. 5(1)(a) GDPR.

⁹⁴ Art. 13(2)(f) and 14(2)(g) GDPR. For more information on this, see Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (6 February 2018), available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, and Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679* (11 April 2018), available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

⁹⁵ See Section 2.3.2.2, above. It should be noted that data subjects must be informed by controllers of the purposes for which personal data are to be processed, under Arts. 13(1)(c) and 14(1)(c) GDPR; this is also a result of the need for purposes to be explicit, under the principle of purpose limitation, reflected in Art. 5(1)(b) GDPR. For more on this, see Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation* (2 April 2013), available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, and Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679* (11 April 2018), available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

⁹⁶ High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for a trustworthy AI* (8 April 2019), pp. 18, 28-29, available at: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.

⁹⁷ *Ibid*, p. 18.

and traceable to the AI system developer, including, to the extent possible, the hypothetical decisions that the AI could make as well.⁹⁸

Explainability, on the other hand, requires an assessment of whether and how decisions made by an AI system are understood, how much AI-made decisions can affect its own decision-making processes, why the system was deployed and what the business model of the system is – in other words, AI-based systems must be designed in a manner which ensures that the systems can be explained to the individuals concerned.⁹⁹ The ICO has also published an in-depth guidance about explainability, which provides the concrete list of six tasks as a systematic approach to both designing AI models in an “explanation-aware” manner and deploying AI systems’ accompanied by explanations fitting to the different audiences at hand.¹⁰⁰ The first task asks for organisations to prioritise the rationale of explainability from the design stage, also by understanding the sector and context that the AI model will be deployed, which can shed light into people’s expectation of the content and scope of similar explanations (if any exist).¹⁰¹ The second task involves the careful selection, collection and pre-processing of data in a way that will empower the organisation to later provide information for the rationale explanation; while the third task provides the details on how to extract explanations from the AI system and ensure that different explanation models can be used.¹⁰² The fourth task brings together the assessments, choices, and lead to the ‘translation’ of the technical rationale of the AI’s systems’ results into easily comprehensible reasons. Interestingly, the fifth step involves the education of the ‘human in the loop’ (in short, implementer) and also possibly suggest more holistic considerations than the technical experts may have concluded to in the fourth task. Finally, the actual building and presentation of the explanation must consider all the factors of delivering an explanation.¹⁰³ All in all, it is worth noting that the ICO has made vast progress in providing a solid framework to AI model architects and developers to comply with the requirement of explainability introduced by the High-Level Expert Group on Artificial Intelligence.

The third requirement for transparency is communication and it entails the use of a disclaimer when deploying AI systems.¹⁰⁴ The disclaimer should not only allow individuals to understand that they are interacting with an AI system as opposed to a human being but should also directly communicate to the individuals concerned the risks inherent to the AI system (e.g., discrimination, impact in economic situation, bias, etc.).

One specification of the issue of transparency with regards to the information that must be shared with the individual concerned, involves the principle of lawfulness, and more precisely the selection of an appropriate legal basis for the use of AI. Controllers wishing to rely on AI systems to carry out automated individual decision-making will

⁹⁸ *Ibid.*

⁹⁹ *Ibid.*, p. 29.

¹⁰⁰ Guidance on Explaining decisions made with Artificial Intelligence, Information Commissioner’s Office and The Alan Turing Institute, Part 2: Explaining AI in practice, available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/explaining-decisions-made-with-artificial-intelligence/part-2-explaining-ai-in-practice/>.

¹⁰¹ *Ibid.*

¹⁰² *Ibid.*

¹⁰³ The ICO identifies five main factors, including the domain factor, impact factor, data factor, urgency factor and audience factor. Although these have been already considered previously, they must play an important role in the final decision on how the explanation will be delivered, when, and what will be included within it.

¹⁰⁴ See High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for a trustworthy AI* (8 April 2019), p. 29, available at: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.

not only have to identify a legal basis, under Art. 6 GDPR, but must also ensure that an exception, under Art. 22(2) GDPR, applies to their specific case. In particular, in the absence of Union or Member State law authorising the use of AI in this manner, controllers will be met with a choice: either Art. 22(2)(a) GDPR¹⁰⁵ is applicable, and therefore, they must rely on Art. 6(1)(b) GDPR,¹⁰⁶ or Art. 22(2)(c) GDPR¹⁰⁷ is applicable, and therefore, they must rely on explicit consent from the data subjects concerned.

However, both of these options represent particular challenges: Art. 6(1)(b) GDPR requires the processing in question to be objectively necessary for either the performance of a contract with a data subject, or to take pre-contractual steps at the data subject's request – if realistic and less intrusive options can be relied on to do so, this legal basis cannot be relied on;¹⁰⁸ consent, in turn, must be informed, which requires a minimum amount of information to be provided to data subjects about the processing to which they are consenting – naturally, if the processing purposes change, or other substantial parts of the information provided change, the validity of the consent itself may be called into question.¹⁰⁹ Outside of the scope of Art. 22 GDPR (such as where the decisions made do not create a legal or similarly significant effect on individuals, including, e.g., for the performance of analytics which are not used to make decisions on individuals,¹¹⁰ or where there is substantial human intervention in an AI-based decision-making process¹¹¹), controllers may consider other legal basis, including the pursuit of legitimate interests under Art. 6(1)(f) GDPR – this, however, will require a comprehensive legitimate interests assessment.

The challenges faced by AI in terms of transparency and lawfulness can be seen as sharing similarities with the processing of personal data for scientific research purposes – as noted by Recital 33 GDPR, *“[i]t is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to*

¹⁰⁵ Art. 22(2)(a) GDPR allows the processing of personal data in connection with automated individual decision-making if this is “*necessary for entering into, or performance of, a contract between the data subject and a data controller*”.

¹⁰⁶ Art. 6(1)(b) GDPR allows the processing of personal data, in general, if this is “*necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract*”.

¹⁰⁷ Art. 22(2)(c) GDPR allows the processing of personal data in connection with automated individual decision-making if this is “*based on the data subject's explicit consent*”.

¹⁰⁸ European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects (8 October 2019), p. 8, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf.

¹⁰⁹ Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679 (10 April 2018, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051), p. 18: “*(...) controllers do need to obtain a new and specific consent if purposes for data processing change after consent was obtained or if an additional purpose is envisaged*” and p. 21: “*There is no specific time limit in the GDPR for how long consent will last. How long consent lasts will depend on the context, the scope of the original consent and the expectations of the data subject. If the processing operations change or evolve considerably then the original consent is no longer valid. If this is the case, then new consent needs to be obtained*”.

¹¹⁰ For more examples of decisions which may, or may not, produce a legal or similarly significant effect on data subjects, see Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (6 February 2018), pp. 21-22, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

¹¹¹ Note that, where such substantial human intervention exists, the decision-making process can arguably be excluded from the scope of Art. 22 GDPR (as it is no longer fully automated). On this, see Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, p. 30 (6 February 2018, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053).

certain areas of scientific research when in keeping with recognised ethical standards for scientific research". This Recital goes on to suggest that data subjects should have the opportunity to give their consent "*only to certain areas of research or parts of research projects to the extent allowed by the intended purpose*".¹¹²

Inspired by this Recital, an innovative suggestion would be to **develop guidance and/or other means for AI developers and users to have the ability to provide dynamic information notices (using illustrations, flowcharts, videos, etc.) to data subjects, seeking to inform them about the key aspects of how their personal data will be used, walking them through the AI's process step-by-step and, where relevant, asking for their consent to the parts of the processing which are known at the time** – this information and consent request could then be updated/renewed in the case of any foreseen substantial changes at a later stage. However, in order for this to function in a manner similar to the possibility foreseen by Recital 33 GDPR, it is important that the renewal of consent is asked prior to the further processing which relies on it being carried out;¹¹³ this would require developers to design AI systems so that it does not automatically proceed with incompatible further processing of personal data, unless it is confirmed – by the developer or user – that a legal basis for this exists. In addition, **in-depth guidance around the requirement of traceability as introduced by the High-Level Expert Group on Artificial Intelligence, such as the ICO's in-depth guidance on explainability of AI**, would further equip all stakeholders with the necessary tools to tackle the challenges of providing transparent and evidently compliant AI systems and algorithms. As a follow-up to the preliminary recommendation of D3.5, it is highly **recommended to invest in researching initiatives, through the Horizon Europe or Digital Europe Program, that aim to explore further ways to grant transparency – for data subjects – on the logic of the automated processing which regards them**.

It is worth noting that the compliance of "high-risk" AI systems with transparency requirements will be guaranteed through the AIA proposal which will only allow AI systems to be brought into market as long as they have incorporated the acceptable level of transparent and understandability for users of the system, including human oversight.¹¹⁴

¹¹² For more on the applicability of Recital 33 GDPR to the use of consent in connection with scientific research purposes, see Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679* (10 April 2018), pp. 28-30, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

¹¹³ On this, note the position stated in Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679* (10 April 2018, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051), pp. 17-18: "*In any event, consent must always be obtained before the controller starts processing personal data for which consent is needed. WP29 has consistently held in previous opinions that consent should be given prior to the processing activity. Although the GDPR does not literally prescribe in Article 4(11) that consent must be given prior to the processing activity, this is clearly implied. The heading of Article 6(1) and the wording 'has given' in Article 6(1)(a) support this interpretation. It follows logically from Article 6 and Recital 40 that a valid lawful basis must be present before starting a data processing. Therefore, consent should be given prior to the processing activity.*"

¹¹⁴ To be precise, some AI systems which are not classified as high risk would also be subject to specific transparency obligations, albeit in a more limited manner. The benchmark of transparency at the moment is that individuals would at least need to be informed about the existence of an AI system. For more on this aspect see: Art. 52 of the Proposal for A Regulation of The European Parliament and of The Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts COM/2021/206 Final, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>.

Other issues arise specifically around the use of consent, such as the need to allow for consent to be withdrawn.¹¹⁵ Developers must bear this in mind, and design AI-based systems to allow data pertaining to specific individuals to be extracted from a dataset and not further considered by the system in question. **Guidance and further research on how this can be attained in practice – in particular, considering that, where automated individual decision-making is concerned, Art. 22(2)(c) GDPR is, as our practical experience has shown, the most likely exception to be relied on – would be welcomed.**

2.3.2.4 Security and Fairness by Design of Security

Security of datasets used in AI-based systems is a key concern.¹¹⁶ There are several ways in which these datasets can be maliciously compromised, such as proprietary hacking of datasets, or even use of datasets against the AI in order to disrupt its decision-making.¹¹⁷ Where machine-learning is concerned, the fact that such systems can autonomously deviate from their originally programmed goals can lead to the choices and predictions generated by such systems being misled by an attacker. The impact of an integrity attack on a dataset, or on an AI processing such a dataset, can be massive, and could trigger public interest concerns – consider, for example, where hacking a connected vehicle could put people's lives at risk. Security measures applied to AI must consider the direct risk that attacks on AI or its dataset may create for individuals.

In order to determine and implement appropriate security measures, AI developers and users must necessarily assess the relevant risks involved, so that they can select those measures deemed most adequate to address them. This refers to the risk-based approach promoted by the GDPR (in particular, for this case, Art. 32 GDPR), but which is also addressed in the NIS-D – the NIS-D expects OESs and DSPs (including those using AI) to manage the risks posed to their networks and information systems, through the implementation of appropriate security measures. If proper risk management is not carried out, then both the GDPR and NIS-D are breached. Based on our experience in the Cyberwatchin.eu project the way it appears best to resolve this issue is **the development of further clear and understandable guidelines for AI developers and users on (1) AI risk management, and (2) examples of security measures, at varying levels of sophistication (to account for developers and users of different sizes, types and economic capabilities), which may be considered in order to properly address identified risks.**

Concerning use of AI and the NIS-D, one key reference to make is to the concept of SIEM (security information and event management), which indicates a model of approach to risk management combining two fundamental functions: (1) SIM (security information management) and (2) SEM (security event management). The key principle underlying any SIEM software solution is the ability to aggregate significant data from multiple sources, to identify deviations/anomalies from the norm, and then trigger appropriate actions to solve the security problem (e.g., when a potential critical event is identified, a SIEM solution can gather additional information, generate alarms and indicate additional security controls to block the progress of that event). By collecting and aggregating information from, e.g., servers, physical/virtual storage

¹¹⁵ Art. 7(3) GDPR.

¹¹⁶ For more on this, see, e.g., Jake Saper, *How to Hack Your Way Into a Proprietary Data Set* (17 July 2018), available at: <https://www.forbes.com/sites/insights-intelai/2018/07/17/how-to-hack-your-way-into-a-proprietary-data-set/>.

¹¹⁷ For more on this, see, e.g., Florian Tramèr et al, *Stealing Machine Learning Models via Prediction APIs* (August 2016), available at: https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_tramer.pdf.

resources, PCs and smartphones, SIEM solutions essentially help to keep the various security measures which may be at a developer or user's disposal manageable. SIEM software can use heuristic algorithms that contemplate the probability of addressing cyber-attacks of various types, such as zero-day exploits, distributed denial of service (DDOS) attacks and brute force attacks. The system exploits a baseline, a basic model that allows it to perform pattern matching operations, log aggregation and analysis to locate anomalous activities. A solution of this importance can only be considered fundamental, in combination, in the most complex realities or more compliant with the requirements of the NIS-D, with the presence of a SOC (Security Operation Center).

When applied to the processing of personal data, the principle of fairness requires organisations to assess whether the processing activities they carry out (or intend to carry out) are balanced and proportionate, in the sense that those organisations' interests are reasonably weighed against the reasonable interests and expectations of data subjects with reference to their individual privacy. In this sense, compliance with the principle of fairness must be seen as going beyond legal compliance and, additionally, taking ethical dimensions of data protection into consideration.¹¹⁸

To achieve this in a real and practical sense, organisations must be weighing the interests and expectations of data subjects against their own already when designing their intended AI-based solutions/systems, or when considering the purchase of such solutions/systems. In is in this manner, as a further specification of the concept of data protection by design, that organisations must adhere to the concept of Fairness by Design. An approach mediated by **Fairness by Design** will allow organisations to identify and implement measures to ensure that the processing activities inherent to the use of AI-based solutions/systems do not unreasonably intrude upon the privacy, autonomy and/or integrity of the concerned individuals (in particular, by not exerting undue pressure on individuals to provide personal data, or more personal data than strictly needed for the processing activities to be performed).¹¹⁹

In essence, applying the concept of **Fairness by Design** is a result-oriented exercise: it will be met if the end-result in a processing activity is balanced and proportionate data processing.¹²⁰ Practical applications can include **performing assessments and introducing oversight processes to avoid unfair bias in datasets and algorithms**.¹²¹ On this point, and in order to further emphasise the importance of ethical considerations (and not just mere legal compliance) in the development of AI-based solutions, **further research and the development of clear, understandable and practical guidelines developing the concept of Fairness by Design**

¹¹⁸ Paolo Balboni, *Big Data, Smart Data, My Data, Your Data: Smart Data Protection by Design (Part 4)* (25 October 2018), available at: <https://www.paolobalboni.eu/index.php/2018/10/25/big-data-smart-data-my-data-your-data-smart-data-protection-by-design-part-4/>.

¹¹⁹ See Paolo Balboni, *The Automated Vehicle Safety Consortium and Fairness by Design* (8 May 2019), available at: <https://www.paolobalboni.eu/index.php/2019/05/08/the-automated-vehicle-safety-consortium-and-fairness-by-design/>, which discusses the Automated Vehicle Safety Consortium's efforts to develop a 'product development framework' applicable to manufacturers, developers and integrators of autonomous technologies, which emphasises the importance of "data collection, protection, and sharing required to reconstruct certain events". More information on this is available at: <https://avsc.sae-itc.org/>.

¹²⁰ See, e.g., Paolo Balboni et al, *Legal Aspects of Blockchain Technology: Smart Contracts, Intellectual Property and Data Protection*, in Kuan-Ching Li et al, *Essentials of Blockchain Technology* (Taylor & Francis, 2020).

¹²¹ High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for a trustworthy AI* (8 April 2019), pp. 18, 28-29, available at: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.

(including, for example, a checklist which could be relied on by AI-based solution developers) would be welcomed.

2.3.2.5 Education and training to raise industry awareness

A general recommendation with regards to emerging technologies remains since its identification in the 2nd Concertation Meeting, namely, education and the raising of awareness on the legislation which should be immediately directed to industry players, taking into consideration the size of the entities involved (multinationals, large, medium & small and micro enterprises) as well their sector-specific activities. The data protection challenges discussed above help understand this recommendation further, since they prove that the legislation leaves a gap for uncertainty when it comes to emerging technologies. This recommendation can be considered as referred to both Horizon Europe and DEP. As far as Horizon Europe is concerned, **it is recommended for research initiatives to find the best method to educate the industry operating in the field of emerging technologies on ways to address the existing challenges and give practical instructions on how to concretely achieve compliance.** However, DEP seems to also be able to offer support to address this recommendation, since it plans¹²² to fund advanced digital skills in the context of designing and delivering short-term training and courses for entrepreneurs, small business leaders and the workforce.

2.4 Internet of Things (IoT)

IoT is the second of the Emerging Technologies posing challenges to the European framework for data protection and security of network and information systems we are going to deal with. While the opportunities created for society and, in particular, the economy of having an ecosystem of interconnected services and devices are considerable, the amount of data (including personal data) required by IoT devices/services – collected through a variety of sensors – is both large and intrinsically intrusive for the individuals concerned.¹²³ Considering that ENISA has identified IoT as technology which is “*at the core of operations for many Operators of Essential Services [...] especially considering recent initiatives towards Smart Infrastructures, Industry 4.0, 5G, Smart Grids*”,¹²⁴ ensuring that appropriate security measures can be defined for IoT systems is a matter of particular concern.

¹²² For more details see: https://ec.europa.eu/commission/sites/beta-political/files/budget-june2018-digital-transformation_en.pdf.

¹²³ See, e.g., European Data Protection Supervisor, *Opinion 4/2015 – Towards a new digital ethics* (11 September 2015, available at: https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf), p. 7: “How this information is handled could affect the privacy not only of the users of the devices, including where used in the workplace, but also the rights of others who are observed and recorded by the device. While there is little evidence of actual discrimination, it is clear that the huge volume of personal information collected by the ‘Internet of Things’ is of great interest as a means for maximising revenue through more personalised pricing according to tracked behaviour, particularly in the health insurance sector. Other domain-specific rules will also be challenged, for example where devices involving processing of health data are not be technically categorised as medical devices and fall outside the scope of regulation”. See also, e.g., Mark Hung, *Leading the IoT: Gartner Insights on How to Lead in a Connected World*, available at: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf.

¹²⁴ European Union Agency for Cybersecurity, *Good Practices for Security of IoT* (19 November 2019), p. 7, available at: <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1>.

2.4.1 Challenges remaining

2.4.1.1 Challenges of Data Minimisation

As noted above,¹²⁵ IoT devices and services, as they are generally currently designed, inherently require the processing of large amounts of data (including personal data).¹²⁶ In particular, these devices and services are often configured to allow for communication with other IoT-connected devices and services by default, without needing the intervention or awareness of the data subjects concerned,¹²⁷ which ties this problem into the problem of individuals' potential lack of control over the data which is sent and received by these devices. Just as is the case with AI,¹²⁸ this creates a conflict with the GDPR's principle of data minimisation. As noted by the Article 29 Data Protection Working Party, "[s]ome stakeholders consider that the data minimisation principle can limit potential opportunities of the IoT, hence be a barrier for innovation, based on the idea that potential benefits from data processing would come from exploratory analysis aiming to find non-obvious correlations and trends".¹²⁹

One solution which could be considered by IoT developers/providers is to provide **more comprehensively designed IoT devices and services with the principle of data minimisation in mind**, incorporating the concepts of data protection by design and by default into the development process.¹³⁰ In particular, as has been noted by the Article 29 Data Protection Working Party in the past, the principle of data minimisation "specifically implies that when personal data is not necessary to provide a specific service run on the IoT, the data subject should at the least be offered the possibility to use the service anonymously".¹³¹ The European Data Protection Board has produced recent guidelines which can act as a helpful checklist in this regard, particularly concerning the principle of data minimisation.¹³² One of the ways in which this could be done, which would also address the problem of individuals' lack of control over IoT data flows, would be for developers to consider **creating 'privacy dashboards'**¹³³ or

¹²⁵ See Sections 1 and 3.2, above.

¹²⁶ See, e.g., European Commission, *IoT Privacy, Data Protection, Information Security* (available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753), p. 1.

¹²⁷ See, e.g., Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things* (16 September 2014), p. 6, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

¹²⁸ See Section 3.1.1, above.

¹²⁹ Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things* (16 September 2014), p. 16, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

¹³⁰ See the Mauritius Declaration on the Internet of Things, issued at the 36th International Conference of Data Protection and Privacy Commissioners (14 October 2014, available at: https://edps.europa.eu/sites/edp/files/publication/14-10-14_mauritius_declaration_en.pdf): "Data processing starts from the moment the data are collected. All protective measures should be in place from the outset. We encourage the development of technologies that facilitate new ways to incorporate data protection and consumer privacy from the outset. Privacy by design and default should no longer be regarded as something peculiar. They should become a key selling point of innovative technologies".

¹³¹ Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things* (16 September 2014), pp. 16-17, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

¹³² See European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* (13 November 2019), in particular pp. 19-20. See also, e.g., UK Information Commissioner's Office, *Data protection by design and by default*, available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/>.

¹³³ Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679* (11 April 2018, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227), pp. 20-21.

‘privacy interfaces’ for individuals¹³⁴ – these dashboards/interfaces, which could be available on specific devices (such as an individual's mobile phone), could act as a control centre for that individual's IoT devices and services, offering information and options concerning data receipt and transmission for each device or service. By default, all data transmissions which are not strictly needed for the device or service to function (regardless of IoT functionalities) should be turned off, and only activated upon an action of the data subject which would meet the GDPR's requirements for consent.¹³⁵ **This is also a problem which could be addressed by policy and regulation, where stricter requirements on data collection and transmission could be enforced on IoT developers. These could include an obligation to build in ‘do not collect’ switches or permissions into IoT devices and services, so that individuals can disable or limit collection and transmission of data before even activating the device or service.**¹³⁶

Other privacy enhancing technologies could be considered, in this respect – consider, for example, the use of ‘attribute-based credentials’ or ‘anonymous credentials’ in the IoT context, by which individuals could selectively authenticate themselves in relation to IoT devices/services, allowing only the collection/transmission of selected data which they find to be appropriate.¹³⁷

2.4.1.2 Challenges of Data Processing Roles

The processing of personal data through IoT-connected devices or services is often carried out by machines managed by different organisations, each of them using computational capacity provided by cloud service developers/providers and that can also involve analytic software programmes supplied by the related vendors.¹³⁸ This exponentially increases the number of parties involved in the data processing activities and the difficulties in clearly allocating data processing roles (controller or processor) to each one; failure to do so correctly may result in misallocation of respective duties and obligations towards the data subjects and towards the competent supervisory authorities.¹³⁹

¹³⁴ See, e.g., Jennifer Kashatus, *Building Privacy into the Internet of Things* (4 August 2015), and Andy Crabtree et al, *Building accountability into the Internet of Things: the IoT Databox model* (27 January 2018), available at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6560684/>.

¹³⁵ In particular, as defined by Art. 4(11) GDPR, consent must be an “unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”. For more information on this, see Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679* (10 April 2018), pp. 15-18, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

¹³⁶ See, e.g., Gilad Rosner et al, *Privacy and the Internet of Things: Emerging Frameworks for Policy and Design*, available at: https://cltc.berkeley.edu/wp-content/uploads/2018/06/CLTC_Privacy_of_the_IoT-1.pdf.

¹³⁷ See European Data Protection Supervisor, *Opinion 5/2018 – Preliminary Opinion on privacy by design* (31 May 2018), pp. 16-17, available at: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf. ENISA has developed a methodology for assessment of privacy enhancing technology maturity, which can be relevant for technology service providers and users looking to implement such measures to address privacy concerns; see European Union Agency for Cybersecurity, *Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies* (31 March 2016), available at: <https://www.enisa.europa.eu/publications/pets>.

¹³⁸ Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things* (16 September 2014), p. 11, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf. See also European Data Protection Supervisor, *EDPS response to the Commission public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy* (16 December 2015), p. 4, available at: https://edps.europa.eu/sites/edp/files/publication/15-12-16_online_platforms_en.pdf.

¹³⁹ Different supervisory authorities have advanced different models for assigning data processing roles to these stakeholders. See, e.g., Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent*

Given the variety of data processing roles which these stakeholders may play (which may vary per activity),¹⁴⁰ the contractual tools offered by the GDPR, in isolation, arguably do not suffice to address this problem, even if stakeholders would agree to use them to regulate their data processing relationships: joint controllership arrangements, under Art. 26 GDPR, would only cover instances of joint controllership¹⁴¹ between stakeholders, whereas data processing agreements, under Art. 28(3) GDPR, would only cover instances where one stakeholder can be qualified as acting as a processor on behalf of another. A data processing role should be defined for each specific data processing activity or operation performed by an organisation, and not merely adopted wholesale. From the practical experience of the authors, it emerges that many service providers, particularly in the digital and cloud domains, tend to qualify themselves generally as processors on behalf of their clients (which may be correct, concerning processing activities performed on clients' behalf, such as those needed to provide the service in question), when in fact they also perform processing activities for their own purposes (such as running analytics on use of their service, for service development purposes) or for those of third parties (such as engaging in programmatic advertising exchanges within their service). In particular, the GDPR does not provide any express obligations to contractually regulate instances where stakeholders may be acting as autonomous controllers,¹⁴² which may lead to the creation of "grey areas" where each stakeholder feels that the responsibility for compliance lies with another, and thus feels free to process personal data in any ways deemed convenient or beneficial, to the detriment of the individuals concerned. To address this, stakeholders could (and should) consider engaging each other through more complex contractual frameworks (which can be conventionally called "**Data Management Agreements**"), identifying the specific data processing activities/relationships which take place between them and their respective roles for

Developments on the Internet of Things (16 September 2014), pp. 11-13, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, and European Data Protection Supervisor, *EDPS response to the Commission public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy* (16 December 2015), p. 5, available at: https://edps.europa.eu/sites/edp/files/publication/15-12-16_online_platforms_en.pdf.

¹⁴⁰ On this, see Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"* (16 February 2010, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf), p. 25: "(...) the role of processor does not stem from the nature of an entity processing data but from its concrete activities in a specific context. In other words, the same entity may act at the same time as a controller for certain processing operations and as a processor for others, and the qualification as controller or processor has to be assessed with regard to specific sets of data or operations", and European Data Protection Supervisor, *EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725* (7 November 2019, available at:

https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf), p. 11: "(...) one or a set of processing operations may be linked to the concept of controllership. According to a literal interpretation of the Regulation, each action (collection, storage, analysis, disclosure etc.) is a distinct processing operation. In practice, processing operations are grouped in sets of processing operations that serve a defined purpose. Controllers have a certain margin of appreciation in defining the boundaries of sets of processing operations. (...) The exercise of control by a specific actor may apply to the entire processing, but may also be limited to one of its specific operations".

¹⁴¹ Under Art. 26(1) GDPR, "[w]here two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers".

¹⁴² Autonomous controllership exists, generally, where two controllers engage in a processing relationship, each one for their own specific purposes and in a manner that renders them unable to influence the purposes of which the other will further process personal data (as opposed to joint controllership, where the purposes and means of processing are jointly defined by the controllers involved).

each one,¹⁴³ and agreeing on different sets of terms to regulate each category of activity/relationship: (1) controller-to-processor terms, including the minimum obligations of Art. 28(3) GDPR,¹⁴⁴ (2) joint-controllership terms, including the minimum requirements of Art. 26 GDPR,¹⁴⁵ and (3) controller-to-controller terms, regulating aspects such as the provision of information to data subjects on data transmissions performed, responsibility for ensuring lawful collection and transmission of data, restrictions on further processing of data received, cooperation in the event of personal data breaches or supervisory authority requests, etc. Through these data management agreements, stakeholders could establish a level playing field for IoT-collected and -shared data, create greater certainty between them as to the extent to which such data may be used by themselves and others, and thereby create greater assurances of lawful processing for data subjects.

In this respect, **any guidance or further research into the key aspects to be regulated between stakeholders, via Data Management Agreements (in particular, where the controller-to-controller terms are concerned), would be welcomed, to provide tools for stakeholders to effectively self-regulate.**

2.4.1.3 Challenges of Purpose Limitation

Given the interactions possible between different IoT-connected objects and services, multiple data flows may be generated that will, frequently, be left outside of individuals' control. As noted by the Article 29 Data Protection Working Party, *"[i]n the absence of the possibility to effectively control how objects interact or to be able to define virtual boundaries by defining active or non-active zones for specific things, it will become extraordinarily difficult to control the generated flow of data. It will be even more difficult to control its subsequent use, and thereby prevent potential function creep"*.¹⁴⁶ The

¹⁴³ This builds upon the recommendation made by the European Data Protection Supervisor in its *EDPS response to the Commission public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy* (16 December 2015, available at: https://edps.europa.eu/sites/edp/files/publication/15-12-16_online_platforms_en.pdf), p. 5: "The most effective regulatory response, in the above respect, consists of applying in a coherent way the Data Protection Directive, which identifies the controller as 'the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data' and assigns to it the fulfilment of a number of duties designed to protect the individual's rights to privacy and data protection. Therefore, before engaging into any data processing, platform operators and other service providers should identify themselves as data controllers (or joint controllers) in the information they provide to users whose data they process. They can identify their position as controllers based on the mere fact that they are processing personal data for their own purposes. This approach ensures that businesses act responsibly and in compliance with the Directive and that liability is efficiently allocated".

¹⁴⁴ Art. 28(3) GDPR lays down various minimum obligations which must be included in written data processing agreements entered into between controllers and processors, including the need for processors to handle personal data under controller instructions (Art. 28(3)(a) GDPR), implement appropriate security measures (Art. 28(3)(c) GDPR), respect the GDPR's rules on engagement of further processors (Art. 28(3)(d) GDPR), delete or return data processed on behalf of the controller upon termination of the processing (Art. 28(3)(g) GDPR) and, in general, assist the controller in the performance of the controller's obligations (Arts. 28(3)(e), (f) and (h) GDPR).

¹⁴⁵ Art. 26(1) GDPR requires joint controllers to determine their respective responsibilities for GDPR compliance in a transparent manner (particularly where the provision of information to data subjects, and the addressing of data subject requests, is concerned) by means of an arrangement between them, unless this is already legally and specifically regulated.

¹⁴⁶ Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things* (16 September 2014), p. 6, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf. See also European Commission, *IoT Privacy, Data Protection, Information Security* (available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753), p. 2:

"Repurposing of data / mission creep challenge is amplified in an IoT environment – Due to the proliferation of increased amounts of data in an IoT environment, the existing challenge that data will be

European Data Protection Supervisor has also noted that “[t]he interaction between IoT and big data may pose risks to data protection among others, because it allows establishing connections between seemingly isolated and unrelated information. In addition, generating knowledge from trivial data or even data previously thought to be ‘anonymous’ will be made easier by the proliferation of sensors, revealing specific aspects of individual’s habits, behaviours and preferences”.¹⁴⁷ In this sense, similarly to AI,¹⁴⁸ personal data may be further processed by the different stakeholders involved in the development and provision of IoT devices and services, for purposes which may be incompatible with the original purposes motivating the collection of personal data.

Here, again, **the imposition of limitations or further requirements on subsequent processing of personal data, collected and shared between IoT-connected devices and services, seems to be a reasonable solution. Providing individuals with control over which data may be collected and transmitted, through the use of dashboards, privacy centres or other privacy enhancing technologies,**¹⁴⁹ **would already be a large step to achieve this goal.** However, one core difference between the AI systems previously analysed and the problem faced with IoT is the multiple different stakeholders which may be involved in the data collection and sharing process, without necessarily having agreed to any specific terms on how data shared with and received from other stakeholders should be used. In this respect, **imposing contractual limitations between stakeholders (through Data Management Agreements)**¹⁵⁰ **on the further processing of received personal data could be a key step to ensuring that appropriate limitations are in place, particularly in the absence of stricter and clearer policy on IoT data collection, sharing and repurposing.**

2.4.1.4 Challenges of Transparency and Lawfulness

The pervasive nature of IoT data processing can effectively lead to situations where individuals (whether or not they are the end-users or owners of IoT-connected devices) find themselves under third-party monitoring, regardless of whether they are aware of this or not.¹⁵¹ Moreover, where decisions can be taken by IoT-connected devices automatically, individuals will effectively lose control of their personal data in the absence of clear information on the processing activities undertaken by such devices.¹⁵² In more complex IoT systems, there may be no clear and comprehensive point of information where individuals can understand the terms under which their personal data are processed. This, in turn, can affect the validity of legal bases relied

used for purposes in addition or other to those originally specified becomes even more serious to consider. Repurposing of data can be in the cards even before data collection begins, e.g. law enforcement authorities or intelligence agencies may seek access to data collected by others for specified purposes. This is not just in relation to the violation of individual rights to privacy but also may impact on wider social and public acceptance.”

¹⁴⁷ European Data Protection Supervisor, *EDPS response to the Commission public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy* (16 December 2015), p. 4, available at: https://edps.europa.eu/sites/edp/files/publication/15-12-16_online_platforms_en.pdf.

¹⁴⁸ See Section 3.1.2, above.

¹⁴⁹ See Section 3.2.1, above.

¹⁵⁰ See Section 3.2.2, above.

¹⁵¹ Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things* (16 September 2014), p. 6, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

¹⁵² European Commission, *IoT Privacy, Data Protection, Information Security*, p. 4, available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753.

on by IoT developers, such as consent¹⁵³, as well as the ability for individuals whose data is processed to exercise their rights under the GDPR¹⁵⁴ (as, without knowledge that a processing activity is going on, this becomes impossible). As noted above,¹⁵⁵ this runs afoul of the GDPR's principle of transparency, and of the concrete obligations to provide information to data subjects within the GDPR.¹⁵⁶ The GDPR requires information on data processing to be served to individuals before processing happens,¹⁵⁷ thereby reinforcing traditional and time-bound conceptions of notice.¹⁵⁸

Nevertheless, controllers can explore several possibilities that will allow them to ensure that their users understand the processing that takes place and remain informed throughout the entire lifecycle of the IoT deployments. **Two suggestions to help comply with the principle of transparency are the use of just-in-time notifications¹⁵⁹ and periodic notifications,¹⁶⁰ which may allow developers to deliver specific and relevant information to individuals at times when they are most likely to be able to apprehend such information.¹⁶¹** Furthermore, as noted

¹⁵³ As noted in Section 3.1.3 above, consent, under Art. 4(11) GDPR, needs to be informed, requiring the provision of a minimum amount of information to the consenting individual in order to be reliable as a valid legal basis.

¹⁵⁴ See Section 2.1, above.

¹⁵⁵ See Section 2.1 and 3.1.3, above.

¹⁵⁶ Arts. 12, 13, 14, 15 and 34 GDPR.

¹⁵⁷ Art. 13(1) GDPR. Art. 14(3) GDPR, which applies only to data collected indirectly (i.e., from sources other than the data subject itself), allows the provision of this information at a later date – information must be provided within a reasonable period after the personal data have been obtained, but at the latest within one month, unless the data is used for communication with the data subject (in which case, information should be provided at the moment of communication, if sooner than the one-month deadline) or for transmission to another recipient (in which case, information should be provided at the moment of first transmission, if sooner than the one-month deadline). For more on this, see Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679* (11 April 2018), pp. 15-16, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

¹⁵⁸ Michael Moran et al, *IoT and GDPR: A Data Convergence that Pits Against the Cautious* (February 2018), available at: <https://microshare.io/wp-content/uploads/2018/02/GDPRWhitepaperFeb2018.pdf>.

¹⁵⁹ Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679* (11 April 2018, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227), p. 21: "A just-in-time notice is used to provide specific 'privacy information' in an ad hoc manner, as and when it is most relevant for the data subject to read. This method is useful for providing information at various points throughout the process of data collection; it helps to spread the provision of information into easily digestible chunks and reduces the reliance on a single privacy statement/ notice containing information that is difficult to understand out of context. For example, if a data subject purchases a product online, brief explanatory information can be provided in pop-ups accompanying relevant fields of text. The information next to a field requesting the data subject's telephone number could explain for example that this data is only being collected for the purposes of contact regarding the purchase and that it will only be disclosed to the delivery service."

¹⁶⁰ Jennifer Kashatus, *Building Privacy into the Internet of Things* (4 August 2015), available at:

<https://www.technologysleage.com/2015/08/building-privacy-into-the-internet-of-things/>.

Periodic notifications are more persistent and regular reminders about the ongoing data collection that occurs; these are referenced also by the Article 29 Data Protection Working Party in their *Opinion 2/2010 on online behavioural advertising* (22 June 2010, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf), p. 18: "(...) the Article 29 Working Party considers it essential for ad network providers to find ways to inform individuals periodically that the monitoring is taking place. Unless data subjects are given clear and unambiguous reminders, by easy means, of the monitoring, it is quite likely that after a certain period of time, they may not longer be aware that it is still taking place and that they consented to it. In this regard, the Article 29 Working Party would be very supportive of the creation of a symbol and related messages that would alert consumers that an ad network provider monitors their user browsing behaviour for the purposes of serving targeted advertising. This symbol would be very helpful not only to remind individuals of the monitoring but also to control whether they want to continue or revoke their consent."

¹⁶¹ For example, during updates of the IoT device, or other major processes occurring during the lifecycle of the device.

above,¹⁶² **the development of privacy dashboards or control centres for individuals may be fundamental in this respect**, as it can allow not only the creation of a central point where information on the processing activities undertaken may be accessed, but also where individuals may set their preferences in regards to data collection/transmission and, potentially, also exercise their rights under the GDPR directly (e.g., accessing, rectifying, deleting or exporting personal data captured by IoT-connected devices). In any case, **further research and guidelines on effective means by which information on processing activities carried out via IoT can be delivered to individuals – particular those who may be captured by the sensors of such devices, without necessarily owning them or having activated them (such as visitors or passers-by) – would be welcomed.**

2.4.1.5 Challenges of Security

An additional concern of relevance to the use of IoT is the ensuring of end-to-end security during the entire data lifecycle. This is of particular importance given the multiple stakeholders which may be involved, resulting in IoT-connected devices performing data processing under the control of different organisations, without an overarching orchestration and control over the data.¹⁶³ This raises several concerns not only under the GDPR's principle of security, but also under the NIS-D.

First and foremost, it is particularly difficult to ensure the carrying out of regular monitoring, auditing and testing activities where a large number of IoT devices are involved in the processing of information within a system.¹⁶⁴ Auditing may become impractical and unrealistic when considering smart infrastructures, made up of hundreds or even thousands of IoT-connected devices within a certain region; however, failing to audit creates a great amount of exposure to risk, as an attack on one device may result in an attack on the entire IoT-connected network or system. One of the most significant and unfortunately continuously expanding attacks of the IoT ecosystem is DDoS (Distributed Denial of Service), which exploits the vulnerabilities of the protocol related to IoT to perpetrate, more often, systemic attacks.¹⁶⁵ There are also new vulnerabilities found that are related to the use of the Constrained Application Protocol (CoAP). **In light of this, further research and the development guidelines and procedures to assist controllers in carrying out regular monitoring and**

¹⁶² Section 3.2.1, above.

¹⁶³ See, e.g., Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things* (16 September 2014, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf), p. 9: "IoT devices and platforms are also expected to exchange data and store them on service providers' infrastructures. Therefore the security of the IoT should not be envisioned by considering only the security of the devices but also the communication links, storage infrastructure and other inputs of this ecosystem. In the same way, the presence of different levels of processing whose technical design and implementation are provided by different stakeholders does not ensure the adequate coordination amongst all of them and may result in the presence of weak points that can be used to exploit vulnerabilities." On this matter, it is relevant to consider the work performed by ENISA in mapping existing security standards against the IoT landscape: see European Union Agency for Cybersecurity, *IoT Security Standards Gap Analysis* (17 January 2019), available at: <https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis>.

¹⁶⁴ In such a scenario, the heterogeneous connections determine what in information security is technically defined as an "increase of the exposed surface", with an exponential extension of the hardware and software vulnerabilities, connected to potential risks of exploitation by cyber criminals. In such cases, it is not uncommon for IoT devices to be used as proxies and, therefore, the compromise of a device connected to a network inevitably makes all other internal and external resources vulnerable.

¹⁶⁵ DDoS attacks, which can be performed through an increasing proliferation of malware-infected botnets and vulnerable servers that automatically generate further attacks against vulnerable targets, are aimed precisely at disrupting services, which – in the case of essential or digital services – is exactly what the NIS-D seeks to prevent.

testing activities, when faced with systems composed of multiple IoT-connected devices, would be welcomed.

IoT devices, in addition to being hard to monitor, have the ability of communicating with each other. This machine-to-machine communication (M2M) allows them to share certain data in order to improve the IoT and its functionality. However, these M2M capabilities also introduce privacy and cybersecurity concerns across multiple products and services that may be offered, both by OESs and DSPs.¹⁶⁶ Essentially, the interoperability of the M2M can make the entire infrastructure of IoT-connected devices vulnerable.

The European Telecommunications Standards Institute has developed guidelines on cybersecurity in IoT for consumers, which lay out key security concepts which IoT device/service developers and users may consider, in order to address such concerns.¹⁶⁷ Furthermore, an additional consideration would be the

¹⁶⁶ Ellyne Phneah, *M2M Challenges Go Beyond Technicalities* (19 June 2012), available at: <http://www.zdnet.com/article/m2m-challenges-go-beyond-technicalities>.

¹⁶⁷ European Telecommunications Standards Institute, *ETSI TS 103 645 v1.1.1 (2019-02): CYBER; Cyber Security for Consumer Internet of Things* (2019), available at: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf. The main recommendations can be summarised as follows:

- (1) The IoT Devices requires at least one administrative user, that is a user having the ability to operate with elevated privileges inside the IoT Devices (e.g. definition of other users, reset of their passwords).
- (2) The IoT Devices requires the passing of an authentication procedure (e.g. login) before being able to allow the processing of any personal data. This authentication procedure verifies the username and a password of at least of 8 characters in length and containing alphanumeric, special and uppercase characters.
- (3) The IoT Devices requires strong authentication (multi-factor authentication, e.g. possession or biometrics). For IoT Devices that have stateless systems in general, the IoT Devices generates a token to associate to the session. The token associated with the session of the web IoT Devices or stateless systems is sufficiently long (64 or more alphanumeric characters) and impossible to guess. The token associated with the session of the IoT Devices or stateless systems has an expiration time.
- (4) The IoT Devices stores the password within its database in encrypted form.
- (5) The IoT Devices uses a hashing algorithm suitable for password encryption.
- (6) The IoT Devices implements automated password selection restrictions (e.g. a minimum number of characters is set, ignores common or user-referenced passwords). When the user ID is associated to an email address, the IoT Devices requires such email address to be verified. Email addresses associated with a user ID are periodically verified to ensure that the email is still valid and in use.
- (7) The IoT Devices limits or throttles the availability of logins in the event of an abnormal number of unsuccessful access attempts occurring within a short time frame.
- (8) The IoT Devices allows each of its administrative users to assign different permission levels to different users.
- (9) The IoT Devices prevents any non-administrative user from changing the permission levels assigned to other users.
- (10) The IoT Devices protects the data it allows to be processed through pseudonymisation techniques.
- (11) The IoT Devices protects the data that it allows to be processed through transparent encryption techniques. Data processed through the IoT Devices are appropriately classified (e.g. common, particular, judicial, subdivisions in personalized under systems).
- (12) The IoT Devices transmits network traffic in a protected from via state-of-the-art security protocols (e.g. TLS1.2, valid certificates, HSTS). Data processed with the help of the IoT Devices is backed up at least daily. Data processed with the help of the IoT Devices can be restored quickly.
- (13) The IoT Devices is currently supported (e.g. through the release of security updates and patches).
- (14) The IoT Devices is constantly kept up to date. The IoT Devices is periodically subjected to sessions of vulnerability assessment and penetration testing to assert its robustness to cyber-attacks.
- (15) The IoT Devices generates access logs.
- (16) The IoT Devices generates logs of critical actions (e.g. creation or removal of content or users).
- (17) The IoT Devices generates logs of the performed processes.
- (18) The logs are complete, unalterable, are stored for at least six months and the integrity of the logs can be verified. If the IoT Devices is connected with smartphones and requires permissions on the device, it provides policies that describe the purposes of the processing enabled by each permission. If

implementation of end-to-end encryption regarding all data collected and transmitted by and between IoT-connected devices and services.¹⁶⁸ Further security measures and best practices which should be considered include those within **ENISA's guidelines on Good Practices for Security of Internet of Things.**¹⁶⁹

2.4.1.6 Fairness by Design

As noted above,¹⁷⁰ the concept of **Fairness by Design**, as a further specification of the concept of data protection by design, introduces an ethical dimension into the planning and development of processing activities which is fundamental to ensure proper respect for the reasonable expectations and interests of individuals.

Considering IoT-connected devices and services in particular, it is important to additionally bear in mind that the sheer amount of information which may be collected by these devices (which is only exponentiated when multiple such devices/services are connected in a network) may lead to the agglomeration of separate data points on an individual which, when considered jointly, may lead to intensely intrusive mapping of behavioural patterns and profiling.¹⁷¹ Whether or not IoT developers are so inclined,

the IoT Devices is connected with smartphones, it never uses the Device ID as a key to identify a record. If the IoT Devices is for smartphones, it uses certified pinning techniques to avoid MITM attacks. (19) The IoT Devices code does not contain confidential credential components (e.g. passwords, tokens, keys...). The IoT code is developed in accordance with the guidelines for secure code (e.g. CERT, OWASP...).

¹⁶⁸ Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things* (16 September 2014, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf), p. 9: "For example, most of the sensors currently present on the market are not capable of establishing an encrypted link for communications since the computing requirements will have an impact on a device limited by low-powered batteries. With regard to the end-to-end security, the result of the integration of physical and logical components provided by a set of different stakeholders only guarantees the level of security provided by the weakest component." See also, generally, European Union Agency for Network and Information Security, *Good Practices for Security of Internet of Things in the context of Smart Manufacturing* (19 November 2018), p. 37 (PS-10), available at: <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot>.

¹⁶⁹ European Union Agency for Network and Information Security, *Good Practices for Security of Internet of Things in the context of Smart Manufacturing* (19 November 2018), available at: <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot>.

¹⁷⁰ See Section 3.1.5, above.

¹⁷¹ Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things* (16 September 2014, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf), p. 8: "Even though different objects will separately collect isolated pieces of information, a sufficient amount of data collected and further analysed can reveal specific aspects of individual's habits, behaviours and preferences. As seen above, generating knowledge from trivial or even anonymous data will be made easy by the proliferation of sensors, and foster important profiling capabilities. Beyond this, analytics based on information caught in an IoT environment might enable the detection of an individual's even more detailed and complete life and behaviour patterns".

such intensive data collection may have a behaviour-altering effect on individuals,¹⁷² with comparisons having been drawn to CCTV in this regard.¹⁷³

Thus, in the IoT domain, practical applications of this concept include **ensuring that individuals are fully aware and in control of the data collection/transmission carried out by means of IoT-connected devices**,¹⁷⁴ and **implementing inherent restrictions on the amount of data collected and the purposes for which data may be used** (in particular, restricting the 'enrichment' of profiles created on the individual for advertising or other purposes), in the absence of valid consent from the individual him or herself. However, as with AI,¹⁷⁵ in order to ensure that IoT developers and users are bound by ethical considerations in their activities, **further research and the eventual development of clear, understandable and practical guidelines on the concept of Fairness by Design** (including, for example, a checklist which could be relied on by IoT-based solution developers) would be recommended.

3 The fourth Concertation Meeting 2021

The 4th Cyberwatching.eu Concertation meeting of H2020 projects from unit H1 "Cybersecurity & Privacy"¹⁷⁶, as also highlighted in D3.6, included a panel discussion session on the **"Privacy challenges and emerging technologies (AI, IoT, Blockchain)"**. The panel discussion included a group of experts in the field of cybersecurity from different application domain including Dr. Prokopios Drogkaris, a Cybersecurity Expert from ENISA, Mrs. Clemente Vanessa Nunez representing the M-Sec project, Mr. Giannis Giakoumakis representing the PUZZLE project, Mr. Gilad Ezov representing the C4IIOT project, Ms. Kristina Livitckaia representing the nloVe project, Mr. Atta Badii representing the Critical Chains.

¹⁷² Consider, for example, an IoT-connected fridge (which collects information on when it is used and what its contents are), and exchanges this information with an IoT-connected television (which collects information on when it is used and what is watched), to arrive at the conclusion that an individual typically enjoys eating a certain kind of snack when watching a given show at a given hour – the television could display a reminder (or, even more intrusively, an advertisement) to bring that snack into the individual's mind, creating a potential desire to collect that snack from the fridge, or order that snack if it is not "in stock" at his/her fridge. As noted by the European Data Protection Supervisor, *EDPS response to the Commission public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy* (16 December 2015, available at: https://edps.europa.eu/sites/edp/files/publication/15-12-16_online_platforms_en.pdf), p. 7, footnote 8: "Platforms, providers of apps and smart devices may gather data sufficient to build group-specific statistics (corporate-wide profiles or regional profiles) on any users' parameter for themselves or their partners (e.g. corporations or governments). This may create for platforms, service providers and other market players with access to data an incentive to move from supporting users in their self-quantifying (e.g. the possibility offered to users, generally for free, to measure their health parameters) to voluntary smart coaching (e.g. allowing users to follow a healthy lifestyle with advice from a third party) to a phase where they may rely on behavioural scientists to "push" the "right" message onto users at the "right" moment, thus influencing users' behaviour."

¹⁷³ Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things* (16 September 2014, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf), p. 8: "In fact, this trend is likely to have an impact on the way the individual actually behaves, in the same way that it has been demonstrated that the intensive use of CCTV has correspondingly influenced citizen's behaviour in public spaces. With the IoT, such potential surveillance might now reach the most private sphere of the individuals' life, including homes. This will put a pressure on the individual to avoid non-usual behaviour so as to prevent the detection of what might be perceived as anomalies. Such a trend would be very intrusive on the private life and the intimacy of individuals and should be very closely monitored."

¹⁷⁴ This could potentially be achieved, e.g., through the 'privacy dashboards' and 'just-in-time notices' mentioned in Section 3.2.1 and 3.2.4, above.

¹⁷⁵ See Section 3.1.5, above.

¹⁷⁶ <https://www.cyberwatching.eu/news-events/events/brussels-second-cw-concertation-meeting-04062019-0>

In the presentation of Dr. Drogkaris from ENISA the SMEs' concerns with regards to their cybersecurity posture was acknowledged because it is evident that they are not as well-equipped, as opposed to larger organisations, with the means to identify, select and deploy the right technical and organizational measures to increase their organisation's security. It was also highlighted that the term of "risk" may be the same but the goal of a risk assessment differs between the cybersecurity realm and the data protection (GDPR) realm. In the cybersecurity realm the risk assessment targets to protect the assets of the SME, while the data protection risk assessment aims to protect the rights and freedoms of the data subjects. As a result of this complexity, it was **recommended to focus to practical guidance and tools which would infuse the protection of personal data and information security principles into the organization**. Towards this recommendation was also the confirmation that the market is in need of guidelines and good practices to support SMEs, also through certifications or self-attestations.

Further to this direction was the recommendation of **creating compliance assurance tools** through a dynamic citizen-engaged software which would translate the data protection regulations and security requirements for privacy preservation and ethical embedding of solutions. These tools or software would be advantageous for SMEs and any citizen to assess their risk and responsibly implement technological measures.

It is important to emphasize that the most common recommendation from the different experts was to **make "data protection more actionable"**. This would consist of a single of a set of different tools that could a) quickly visualize and understand how an organization should rank their various privacy requirements, b) embed the risk assessment of the processing activities, c) prioritise the various risks, d) explain how to combine the risks with the security aspects, e) help experts understand where the trade-off for compliance should be and accordingly create appropriate security measures.

Another suggestion for policymakers on emerging technologies within the context of European projects was **the need to differentiate the methodology for compliance between the development and deployment of software, products, and tools created through European projects**. To this end, it was suggested that a difference in the guidance should be in place between the development and deployment of solutions that rely on emerging technologies such as AI, IoT, and blockchain.

Finally, experts mentioned the high necessity of creating a dedicated model environment / program that SMEs can use to understand and implement privacy and cybersecurity requirements. This program would require for SMEs to describe the processing activities and product they have created, and the program would become their "broker" on privacy and cybersecurity requirements.

In conclusion, the panel discussion session had a general trend in the suggestions it provided. The experience of the panelists indicated a clear message to the policy makers and supervisory authorities: we have yet to find an actionable way to translate the legal and cybersecurity requirements stemming from the various legislations. A failure to design or develop actionable tools can generate a larger gap between the multinational companies and SMEs. To ensure that the appropriate support is provided, the EU policy makers need to create not only legislations but a comprehensive framework. This means that, potentially, part of the legislative process would include making available practical guidelines, schemes, and implementation tools. The result of such an approach would not only allow for the EU to have a competitive advantage on the implementation of emerging technologies legislation but would truly transform the EU to a legislative innovator.

4 GDPR Temperature Tool 2.0, Information Notice Tool 2.0 and Interactive Webinar with SMEs

The legal compliance of stakeholders is a priority for cyberwatching.eu, and for this reason both tools, the GDPR Temperature Tool and the Information Notice tool have been significantly updated with several new functions put in place.

The GDPR tool is an online self-assessment questionnaire targeting SMEs to facilitate their understanding of where they stand with respect to the GDPR in terms of their “risks to sanctions”. The tool is structured around a set of 16-22 questions (depending on the number of “Yes” or “No” answers the respondent gives) relating to the data processing activities of the company. The different questions tackle a different regulatory requirement or obligation that could lead to sanctions being imposed to the organisation filling out the questionnaire. As can be seen in full detail in Annex A, the GDPR temperature tool touches upon the requirements of special categories of personal data, transparency, consent, minors, automated processing and profiling, data transfers, controller-processor relationships, data protection officers, risk assessments, records of processing activities, and data breach management. The questions remained the same in the 2.0 version of the tool, except for a question on data subject rights which was added.

Following the tool’s success of more than 100 respondents, a 2.0 version was launched in the beginning of 2021. In addition, according to the feedback given by respondents, not only was the tool very easy to use and clearly understandable, but it is also very likely for their organization to use the recommendations, tools or solutions that were suggested. Furthermore, the tool seemed to receive positive feedback with regards to its effectiveness in helping the organization understand their compliance posture and the aspects they need to further assess or work on for a better level of compliance (fitness for purpose). In continuation to the efforts to receive feedback and provide customizable advice according to the organization’s needs, we carried out a dedicated interactive webinar that discussed all the gaps and provided further insights in the recommendations of the tools. The entire slide deck can be found in Annex C. More than the final interactive webinar, throughout the life-time of the cyberwatching.eu project, the legal partners remained active in order to raise awareness of data protection, support the compliance of stakeholders and engage in conversations to understand the needs of the market (especially SMEs) and we have collated all the webinars carried out throughout the project in Annex D.

Each question is accompanied by a set of personalised recommendations based on the different answers a respondent might give. By answering to each question the points towards the organisation’s “Risk of Sanction Level” can increase or decrease. The tool has been complemented in this regard because since the first version many enforcement actions and fines have been imposed by supervisory authorities. These cases of sanctions have helped us better understand the realistic “weight” of requirements and the significance given to them by supervisory authorities. At the end, the respondent receives a valuable report including the recommendations for each question answered, as well as a total “temperature” (green, yellow or red) representing the respondent’s risk of sanction level (low, medium, high, or very high).

Furthermore, the 2.0 version has enhanced the recommendations with two new features. Firstly, the recommendations have been updated with the latest guidance, opinions, and legal best practices, which was published between 2019 and 2021. This guidance also includes an interpretation of the specific framework which arose after the Schrems II decision and the latest EDPB recommendations published in June 2021. Secondly, the recommendations were enhanced by integrating solutions and tools from the cyberwatching marketplace, which help organisations achieve

compliance on the specific aspect the question tackles. These tools were included within a new section called “Additional useful resources, tools and further reading”, which links to various resources and valuable tools developed by supervisory authorities, and ENISA. As a result, the companies filling out the tool will not only get an overview of their strengths and weaknesses in their compliance posture but will also receive immediate recommendations on how to move forward, and suggestions of tools, software, and services they can consider implementing to improve their compliance. Similar updates to recommendations were also carried out to the Information Notice Tool.

The ultimate value of the new recommendations of tool 2.0 is that it collects many available opinions, guidance and tools – acting a repository of knowledge to the SMEs’ availability – and on the other hand distributes online tools, solutions and software that can improve their compliance. It is worth noting that the solutions and tools that were chosen from the cyberwatching marketplace and got embedded in the 2.0 version of the GDPR temperature tool underwent an analysis in order to concretely point out to organisations how they could benefit from them. A summary of this analysis can be found in Annex E R&I Solutions index. Finally, the significance of the tools has also been demonstrated by the Consortium’s decision to exploit the tools in the future by integrating them in the Cyber Digital Innovation Hub. More details on the exploitation strategy can be found in D5.4

5 SUMMARY OF RECOMMENDATIONS

The main recommendations from this document are detailed below.

- **Single Data Protection Space:** need for a single space to collect all the different types of guidance (opinions, guidelines, instruments, tools, self-assessments) created by Supervisory Authorities based on the GDPR ‘topic’ or GDPR ‘obligation’ to ensure easy access availability.
- **Systematic methodology for GDPR risk assessments:** need for the publication of guidelines for organisations, especially in the field of emerging technologies, on methodology to carry out risk assessments. Although this has been partially met by the Spanish Data Protection Authority (AEPD), a more in-depth approach is necessary.
- **Prioritisation of tool creation:** allocation of specific priority areas that require instruments or guidance to different Supervisory Authorities, in order to ensure efficiency and consistency in the guidance provided to organisations.
- **Updated methodology to assess the severity of data breaches and feedback on tool for notification of data breaches:** need for further guidelines on the assessment of the severity of breaches and a methodology on how to manage and react to the breaches. This recommendation could be achieved by updating of the existing methodology from ENISA.
- **European tool for Data Protection Impact Assessment:** the creation of a tool for data protection impact assessments, which could compile the several applicable national black lists, is highly recommended.
- **Guidance on data transfer impact assessments:** further research and guidance on how the assessment prior to data transfers must take place, especially as a result of the Schrems II decision.
- **Data transfer impact assessment tool:** Creation of a data transfer impact assessment tool, similar to the Data Protection Impact Assessment tool created by the French Data Protection Authority, which will assist organisations to assess all

relevant factors and considerations before carrying out data transfers outside the EEA.

- **GDPR and NISD notifications:** Further research on managing notifications that fulfill the requirements of both the NISD and the GDPR.

As far as emerging technologies are concerned:

- **Practical tools:** create a set of practical tools focusing on compliance of emerging technologies, that are kept up to date according to the industry standards and state of art as well as rate of change of the technologies. These practical guidance and tools should also help organisations infuse the protection of personal data and information security principles into their practices. These tools could also include compliance assurance tools and software which would translate the data protection regulations and security requirements for privacy preservation and ethical embedding of solutions.
- **Methodology for development and deployment:** it is necessary to distinguish between the methodology for compliance between the development stage and deployment of software, products, and tools created through European research & innovation projects.
- **Education and training to raise industry awareness:** research initiatives should find the best method to educate the industry operating in the field of emerging technologies on ways to address the existing challenges and give practical instructions on how to concretely achieve compliance.
- **Structured cooperation between policy makers, the research, and the market/industry:** the DEP should aim at drafting a structured flow of information that facilitates the continuous sharing of feedback between policy makers, research initiative and industry on matters regarding emerging technologies.

As far as AI is concerned:

- **Guidelines on methodology for risk analysis specifically related to AI,** which should take into consideration the circumstances that the risk of the processing, as well as the envisaged consequences for data subjects, may not be comprehensively analysed beforehand by the controller, due to the evolving circumstances of the processing activities.
- **Guidelines on AI/machine learning and data minimisation:** it is recommended that policy makers strive for research initiatives that look into how to concretely deploy AI and machine learning models, respect the principle of data minimization, storage limitation and data accuracy (Article 5 (1) (b), (c), (d) GDPR).
- **Guidelines on purpose limitation:** provide clarification, through the Artificial Intelligence Act, the tensions between the GDPR principle of purpose limitation and the training and deployment of AI systems.
- **Guidance for SMEs on methodology on training and implementation:** provide guidance on the methodology that SMEs / start-ups training or implementing AI systems in their processes should follow.
- **Guidance on provision of information relating to AI systems:** guidance and/or other means for AI developers and users to have the ability to provide dynamic information notices (using illustrations, flowcharts, videos, etc.).
- **Guidance on traceability of AI systems and algorithms:** Guidance around the requirement of traceability as introduced by the High-Level Expert Group on Artificial Intelligence.
- **Research on transparency in AI:** Provide opportunities to research initiatives, through the Horizon Europe or Digital Europe Program, to explore further ways to grant transparency – for data subjects – on the logic of the automated processing which regards them.

- **Guidelines on Risk management and appropriate security measures:** Development of further clear and understandable guidelines for AI developers and users on (1) AI risk management, and (2) examples of security measures, at varying levels of sophistication which may be considered to properly address identified risks.
- **Guidelines on Fairness by Design:** Further research and the development of clear, understandable, and practical guidelines developing the concept of Fairness by Design (a checklist which could be relied on by AI-based solution developers).

As far as IoT is concerned:

- **Need for further guidelines on the application of principles of data protection by design/default and data minimisation for IoT deployments:** such guidelines should give advice on how to concretely inform users as per Art.s 12-13-14 GDPR, which legal basis is permitted to process personal data and how data subjects can effectively exercise their rights. Moreover, such guidelines should address end-to-end security during the entire data-lifecycle, given that the machines performing data processing are typically under the control of different organisations (acting as controllers or processors as the case may be) without an overarching orchestration and control over the data.
- **Practical guidelines on the allocation of privacy roles in IoT environments in the light of the GDPR** are needed, since IoT poses strong challenges to the allocation of privacy roles of the several parties involved in processing. The use of data protection contracts (i.e., Privacy Level Agreements) - other than data processing agreements pursuant to Art. 28 or joint-controllership agreements pursuant to Art. 26 GDPR – should be considered, whereby, regardless of the privacy rules, duties, obligations and responsibilities of the parties involved are clearly spelled out.
- **Guidelines on Data Management Agreements:** it is necessary to have further research and guidance into the key aspects to be regulated between stakeholders, via Data Management Agreements (in particular, where the controller-to-controller terms are concerned), to provide tools for stakeholders to effectively self-regulate.
- **Guidelines on information provision:** need for more effective means by which information on processing activities carried out via IoT can be delivered to individuals – particular those who may be captured by the sensors of such devices, without necessarily owning them or having activated them (such as visitors or passers-by).
- **Guidelines on IoT monitoring and testing:** Guidelines and procedures to assist controllers in carrying out regular monitoring and testing activities, when faced with systems composed of multiple IoT-connected devices.
- **Guidelines on Fairness by Design in IoT:** Ensure that IoT developers and users are bound by ethical considerations in their activities, further research and the development of clear, understandable, and practical guidelines developing the concept of Fairness by Design (including, for example, a checklist which could be relied on by IoT-based solution developers) would be welcomed.

ANNEXES

ANNEX A. Survey and recommendations for SMES: the GDPR temperature tool

ANNEX B. Survey and recommendations for information notices

ANNEX C. Presentation slides for GDPR webinar

ANNEX D. Participation at Legal compliance webinars, workshops, round-table discussions, panels

ANNEX E. R&I Solutions index

ANNEX F. Glossary

ANNEX A. SURVEY AND RECOMMENDATIONS FOR SMES: THE GDPR TEMPERATURE TOOL

Q1. Select your geographical scope of operations: *

(drop down menu)

- ⇒ EU organisation operating only in its country
- ⇒ EU organisation operating across EU (two or more EU countries)
- ⇒ Organisation from an associated country (Israel, Turkey, etc.) operating in EU
- ⇒ Non-EU organization operating in EU

For SMEs who are an **EU organisation operating only in its country**, the following recommendation would pop up, and **one point added** to the SMEs' "GDPR Temperature".

"As an entity operating only in one Member State, please be cautious that this Member State may define stricter or at least more specific rules on certain areas of the General Data Protection Regulation. For example, a Member State may:

- maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health, [Art. 9 (4) GDPR]; or
- lower the stipulated age of 16 years old in offering information society services directly to a child, with the lowest limitation at 13 years old [Art. 8 (1) GDPR].
- provide for criminal penalties for infringements of the GDPR or of national data protection laws.

In short: make sure to stay updated with the national laws on data protection, especially looking into the points where the GDPR allows Member States to integrate the GDPR.

For SMEs who are an **EU organisation operating across EU** (two or more EU countries) the following recommendation would pop up, and **two points added** to the SMEs' "GDPR Temperature".

As an entity operating across the entire EU, please be cautious that each Member State may define stricter or at least more specific rules on certain areas of the General Data Protection Regulation. For example, a Member State may:

- maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health, [Art. 9 (4) GDPR]; or,
- lower the stipulated age of 16 years old in offering information society services directly to a child, with the lowest limitation at 13 years old [Art. 8 (1) GDPR].
- provide for criminal penalties for infringements of the GDPR or of national data protection laws.

In short: make sure to stay updated with the national data protection laws of the countries where your company operates, especially looking into the points where the GDPR allows Member States to integrate the GDPR.

For SMEs who are an **organisation from an associated country** (Israel, Turkey, etc.) **operating in EU, or who are a non-EU organisation operating in EU** the following recommendation would pop up, and **three points added** to the SMEs' "GDPR Temperature".

As an entity not established in the E.U., but operating on the entire EU (meaning, processing the personal data of data subjects who are in the Union), the GDPR **may** apply to you where your processing activities relate to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required
- the monitoring of the data subjects' behaviour. [Art. 3 (2) GDPR]

Additionally, if the above conditions apply to your entity, please be cautious that each Member State may define stricter or at least more specific rules on certain areas of the General Data Protection Regulation. For example, a Member State may:

- maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health, [Art. 9 (4) GDPR]; or,
- lower the stipulated age of 16 years old in offering information society services directly to a child, with the lowest limitation at 13 years old [Art. 8 (1) GDPR].
- provide for criminal penalties for infringements of the GDPR or of national data protection laws.

In short: make sure to stay updated with the national data protection laws of the countries where your company operates, especially looking into the points where the GDPR allows Member States to integrate the GDPR.

In addition to the above, **if you are a United Kingdom business or organization and you receive personal data or operates in the EU**, the Information Commissioner's Office ("ICO", the UK's data protection authority) explains that the European Commission is evaluating the granting of an adequacy decision to the UK. The adequacy decision would allow UK businesses and organisations to receive personal data from the European Economic Area (EEA) with similar or the same data protection rules as those that have been implemented until 2020. However, if you are a UK business that receives personal data from the EEA, the ICO recommends taking extra steps to ensure that the data flow will not be affected even if an adequacy decision is not issued by the European Commission. On the other hand, if your organisation has an office or a branch in the EEA, your organization will need to comply with both the UK and the EU data protection regulations; and you may need to designate a representative in the EEA. An important action that you must take is to identify the data you hold in the EU before the end of 2020, the so-called 'legacy data' in order to apply the rules of the GDPR to it. A useful tool to help you decide if you are processing any 'legacy data' is the [End of Transition Interactive Tool](#) by the ICO. However, keep in mind that if the EU Commission grants an adequacy decision to the UK the requirements applied to this legacy data can also change.

In any case, we recommend that you constantly monitor the ICO website [for any updates for SMEs on data protection after the end of the Brexit transition periods](#), as well as the general [news and announcements on data protection after the end of the transition period](#) (for ease, you can also sign up to the ICO newsletter) in order to ensure that you follow the most up-to-date guidance and implement it within your organization in a timely manner.

Additional useful resources, tools and further reading:

Resources, Tools & Solutions:

- [End of Transition Interactive Tool](#) for small businesses by the Information Commissioner's Office (ICO).
- [An interactive tool designed](#) for small and medium-sized businesses and organisations based in the UK who need to maintain the free flow of personal data from Europe to the UK.

Further reading:

The ICO has already made available many different tools for compliance with the post-Brexit requirements that SMEs must be aware of, including:

- [A webinar aimed at SMEs](#) discussing the key data protection requirements to consider at the end of the transition period.
- [Frequently asked questions \(FAQs\)](#) about information rights and the end of the transition period.

Regardless of the answer given, the following recommendation would show up.

Keep in mind that your exposure to GDPR sanctions varies depending on the circumstances of each case, according to Art. 83 GDPR¹⁷⁷; however, it is important to note that for companies, the administrative fine may be up to 2% of your total worldwide annual turnover (for infringements on certain provisions) or even 4% of your total worldwide annual turnover (for infringements on more crucial provisions). The decision on whether to impose an

¹⁷⁷ [Art. 83 GDPR](#).

administrative fine and determining the amount will depend on the following conditions, including:

- The nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned, and the number of data subjects affected, and the level of damage suffered by them;
- The intentional or negligent character of the infringement;
- Any mitigating actions that were taken by the controller or processor in order to minimise the damage suffered by data subjects;
- The degree of responsibility of the controller or processor in mitigating the damage suffered by data subjects (see Articles 25 and 35 GDPR¹⁷⁸);
- Relevant previous infringements by the controller or processor;
- The degree of cooperation with the supervisory authority so that the infringement can be remedied, and possibly mitigate harmful effects of the infringement;
- The categories of personal data affected by the infringement;
- The way with which the infringement became known to the supervisory authority, especially considering if and to what extent the controller or processor directly notified the infringement;
- Compliance with corrective measures previously issued by the supervisory authority against the controller or processor on the same subject-matter under [Art. 58 GDPR](#) (for example, an order to comply with the data subject's request to exercise his / her rights, or a warning that a processing operation is likely to infringe the GDPR, or an order to impose a temporary or definitive limitation such as a ban on processing);
- Adherence to approved codes of conduct (pursuant to [Article 40 GDPR](#)) or approved certification mechanisms ([Article 42 GDPR](#));
- Any other aggravating or mitigating factor applicable to the circumstances of the case, for example, financial benefits gained or losses avoided, directly or indirectly from the infringement.

We recommend using the above conditions as a compass to comprehend the possibility to **both prevent administrative sanctions** against your organization, as well as **to mitigate the extent of the administrative sanction** through proactive behaviour and an overall cooperative approach towards the supervisory authority.

Q2. What is the total annual worldwide turnover of your entity?

For SMEs who have a total annual worldwide turnover between 0 and 150.000 euro, **zero points** would be added to their "GDPR Temperature".

For SMEs who have a total annual worldwide turnover between 150.000 and 500.000 euro, **one point would be added** to their "GDPR Temperature".

For SMEs who have a total annual worldwide turnover between 500.000 and 1 million euro, **two points would be added** to their "GDPR Temperature".

For SMEs who have a total annual worldwide turnover of 1 million euro and above, **three points would be added** to their "GDPR Temperature".

Q3. Does your organisation process special categories of personal data (i.e., sensitive data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation) or judicial data (such as personal data relating to criminal convictions and offences)?

If an SME responded positive to this question, the below recommendation would be proposed, and **five points** would be **added** to their "GDPR Temperature".

Seeing as your company processes special categories of personal data, there are additional obligations expected according to the GDPR. To be more precise, the GDPR stipulates that a data controller is prohibited to process special categories of personal data (such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic or biometric data, or any

¹⁷⁸ [Art. 25](#) and [32 GDPR](#).

data concerning the health or a person's sex life or sexual orientation) unless the data controller follows on one of the legal bases enlisted in article 9(2) of the GDPR.

More generally, if your company does process such special categories of personal data, the main way to do so is if you have received **explicit consent** to the processing of those personal data. Explicit consent will **not be needed** if one of the below applies to you:

- the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the **field of employment and social security** and social protection law (i.e., only to be used in employment relationships, or when related to social security);
- the processing is necessary to protect **the vital interests of the data subject** (i.e., only to be used in life or death situations);
- the processing is carried out by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim- in the course of its **legitimate activities**, and, on condition that the processing related **solely to members, former members**, or to persons regularly contacting the foundation (i.e., a not-for-profit body processes the health data of its members for the purpose of providing them health insurance);
- the processing relates to personal data which are **manifestly made public** by the data subject (i.e., entered their data on a public database provided by a governmental or enforcement authority);
- the processing is necessary for the establishment, exercise or defence of **legal claims** (i.e., when a company must collect such data in order to defend themselves in court proceedings)
- the processing is necessary for the purposes of **preventive or occupational medicine** (i.e., a company that provides medical diagnosis, a company that manages healthcare or social care systems and services, or generally medicine-related companies that may collaborate with health professionals in order to cure a disease or a disorder);
- the processing is necessary for reasons of public interest in the area of **public health** (i.e., a company involved in the protection against serious cross border threats to health)
- the processing is necessary for **archiving purposes in the public interest, scientific or historical research** purpose or **statistical** purposes. (i.e., a research company conducts in-depth research for statistical purposes).

In case none of the above applies to the processing activities your company conducts, "explicit" consent is required. "Explicit" refers to the way consent is expressed by the data subject, meaning that in the case where you collect special categories of personal data, the data subject must give an **express statement** of consent such as in a written statement (where possible), or via an electronic form, through the sending of an email, or by uploading a scanned document which is signed by the data subject.¹⁷⁹ Theoretically, oral statements may also be a way to obtain valid explicit consent, however, at a later stage, it may be difficult to prove that all conditions for a valid consent were met when the statement was recorded.¹⁸⁰

If your organisation uses online software or obtains the personal data online, then two-stage verification of consent may also be a way to make sure explicit consent is valid.¹⁸¹ An example of this method could be for the data subject to receive an e-mail notifying him/her of the controller's intent to process a record containing medical data, for example, and asking for his/her explicit consent. Then, if the data subject agrees to the use of his/her data, he/she will be asked to send an e-mail reply containing the statement "I agree". Once the reply is sent, the data subject will receive a verification link that must be clicked; either in a follow-up e-mail or via SMS with a verification code, to confirm his/her earlier agreement.¹⁸² You are free to choose other methods to obtain explicit consent, however, it is recommended the ones mentioned above were those that have been suggested by the European Data Protection Board (also known as Working Party 29), in their Guidelines on Consent."

¹⁷⁹ Article 29 Working Party Guidelines on consent under Regulation 2016/679, as last Revised and Adopted on 10 April 2018, p. 18.

¹⁸⁰ Article 29 Working Party Guidelines on consent under Regulation 2016/679, as last Revised and Adopted on 10 April 2018, p. 18.

¹⁸¹ Article 29 Working Party Guidelines on consent under Regulation 2016/679, as last Revised and Adopted on 10 April 2018, p. 19.

¹⁸² Article 29 Working Party Guidelines on consent under Regulation 2016/679, as last Revised and Adopted on 10 April 2018, p. 19.

Finally, the Article 29 Working Party has highlighted that one of the criteria for deciding whether a Data Protection Impact Assessment should be carried out is to consider whether 'sensitive data' is processed.¹⁸³ According to the opinion, sensitive data or data of highly personal nature **includes special categories of personal data** as defined in [Article 9 GDPR](#), for example information about political opinions, and personal data relating to criminal convictions or offences as defined in [Article 10 GDPR](#). These categories of personal data may mandatorily require a Data Protection Impact Assessment to be carried out in order to assess the risk being posed to the data subjects and propose mitigating security measures. Therefore, please carefully consider whether it is mandatory to carry out a DPIA according to this criteria.

Additional useful resources, tools and further reading:

Resources, Tools & Solutions:

- [A modular tool to conduct Data Protection Impact Assessment](#), through a step-by-step process, which can also be customised based on the specific needs of an SME or your business sector has been created by the French Data Protection Authority. This software is available in both portal and web versions, and can be found for free here.
- [Self assessment checklist for GDPR Readiness Checklist Tool on legal basis](#) (click on "data security") by the Irish Data Protection Commission.

Further reading:

- [Guidelines 05/2020 on Consent](#) under Regulation 2016/679 Version 1.1, Adopted May 2020.
- [Article 29 Working Party Guidelines on consent](#) under Regulation 2016/679, Adopted on November 2017 as last Revised and Adopted on 10 April 2018.
- [Guide on Special Category Data](#) by the Information Commissioner's Office (ICO).
- [Guidelines on Data Protection Impact Assessment \(DPIA\)](#) and determining whoever processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.
- [Guide on Data Protection Impact Assessments](#) by the Irish Data Protection Commission.

The methodology of the French Data Protection Authority (CNIL) is a collection of three guides:

- [Privacy Impact Assessment \(PIA\) Methodology](#), which sets out the approach for carrying out a Data Protection Impact Assessment.
- [Privacy Impact Assessment \(PIA\) Templates](#), including information that can be used to carry out the analysis of the Data Protection Impact Assessment.
- [Privacy Impact Assessment \(PIA\) Knowledge Bases](#), a catalogue of controls aimed at complying with the legal requirements and mitigating the risks.

A negative response to this question would **add zero points** to their "GDPR Temperature".

If the answer to Q3. is yes:

Q3B. Does your entity process *genetic data, biometric data, or data concerning health*?

If an SME responded positive to this question, the below recommendation would be proposed, and **one point would be added** to their "GDPR Temperature".

Keep in mind that the Member State where you operate may maintain or introduce **further conditions**, or limitations, with regard to the processing of *genetic data, biometric data, or data concerning health*. Furthermore, remember to always specify in your privacy policy that you process this type of data, indicating one of the legal grounds provided for by art. 9(2) GDPR.

Lastly, the Article 29 Working Party has highlighted that one of the criteria for deciding whether a Data Protection Impact Assessment should be carried out is to consider whether 'sensitive data' is processed.¹⁸⁴ According to the opinion, sensitive data or data of highly personal nature includes special categories of personal data as defined in [Article 9 GDPR](#). For example, if a general hospital keeps patients' medical records, this would require a Data Protection Impact Assessment to be carried out in order to assess the risk being posed to

¹⁸³ Guidelines on Data Protection Impact Assessment (DPIA) and determining whoever processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, pg. 9.

¹⁸⁴ Guidelines on Data Protection Impact Assessment (DPIA) and determining whoever processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, pg. 9.

the data subjects and propose mitigating security measures. Therefore, please carefully consider whether it is mandatory to carry out a DPIA.

Additional useful resources, tools and further reading:

Resources, Tools & Solutions:

- [A modular tool to conduct Data Protection Impact Assessment](#), through a step-by-step process, which can also be customised based on the specific needs of an SME or your business sector has been created by the French Data Protection Authority. This software is available in both portal and web versions, and can be found for free here.
- [Self assessment checklist for GDPR Readiness Checklist Tool on legal basis](#) (click on “data security”) by the Irish Data Protection Commission.

Further reading:

- [Guidelines on Data Protection Impact Assessment \(DPIA\)](#) and determining whoever processing is “likely to result in a high risk” for the purposes of Regulation 2016/679.

The methodology of the French Data Protection Authority (CNIL) is a collection of three guides:

- [Privacy Impact Assessment \(PIA\) Methodology](#), which sets out the approach for carrying out a Data Protection Impact Assessment.
 - [Privacy Impact Assessment \(PIA\) Templates](#), including information that can be used to carry out the analysis of the Data Protection Impact Assessment.
- [Privacy Impact Assessment \(PIA\) Knowledge Bases](#), a catalogue of controls aimed at complying with the legal requirements and mitigating the risks.

If an SME responded negatively to this question, then **zero points** would be added to their “GDPR Temperature”.

Q4. Does your entity provide information to individuals (see [Articles 12, 13](#) and [14 GDPR](#)) prior to processing their personal data (i.e. information notice, privacy policy, etc.)?

If an SME responded with a positive answer to this question, the below recommendation would be proposed, and **zero points** would be added to their “GDPR Temperature”.

Providing an information notice to your data subjects is a great start! However, due to the importance of these communications, we have created a further tool that you can use in order to ensure that your privacy policy is compliant with the GDPR. If you would like to receive further recommendations, or simply check your information notice’s compliance to the GDPR click [here](#)¹⁸⁵ to be transferred to the additional short survey.

Additional useful resources, tools and further reading:

Resources, Tools & Solutions:

- [Information Notice Tool](#) created by Cyberwatching.eu.
- [Self assessment checklist for GDPR Readiness Checklist Tool on legal basis](#) (click on “transparency requirements”) by the Irish Data Protection Commission.
- [Writing a GDPR-compliant privacy notice](#) (template included) by the EU Project gdpr.eu.

Further reading:

- [Guidelines on Transparency under Regulation](#) 2016/679, by Article 29 Working Party, as last Revised and Adopted on 11 April 2018.

If an SME responded with a negative answer to this question, the below recommendation would be proposed, and **four points** would be added to their “GDPR Temperature”.

As an entity that processes personal data of data subjects, you have the obligation to inform your data subjects, **at the time when the personal data are obtained**, of specific aspects of the processing activity. The most valuable information that must be communicated to the data subject is:

- ☐ the identity and contact details of your entity (as a data controller)

¹⁸⁵ The link will lead to the [Information Notice Tool](#).

- ☐ the contact details of your data protection officer (in case a DPO has been designated)
- ☐ the specific **purpose** of the processing
- ☐ the **recipients** or categories of recipients of their personal data
- ☐ the **period** that their personal data will be stored
- ☐ whether the personal data will be transferred outside of the European Union
- ☐ the data subject rights (right to access to and rectification or erasure of their personal data, or the right of restriction of processing or right to object to the processing)
- ☐ The source from which the personal data originates (in case the data was not obtained from the data subjects)¹⁸⁶.

Additionally, it is not enough to simply provide some information about the processing of personal data, therefore we recommend that the information that you do choose to provide is also: 1) concise, transparent, intelligible and easily accessible; 2) written in clear and plain language, particularly if addressed to a child; and 3) free of charge.¹⁸⁷

Lastly, if you process the personal data based on the consent of the individual, then this consent should be freely given, specific, informed (as per the information described above) and an unambiguous indication of the data subject's intention. The consent should be done by a clear **affirmative action** or by a statement that is specific to the processing of personal data relating to him or her.

If this information is not provided, your company is open to a great risk that may result to a data subject sending a complaint to the supervisory authority, which will likely conduct an investigation into the processes of your company. Any infringements on the data subject's right to be informed about the processing of their personal data can be subject to administrative fines up to 20 000 000 euros or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

If you would like to receive further recommendations, or simply check your information notice's compliance to the GDPR click [here](#) to be transferred to the additional short survey we have compiled.

Additional useful resources, tools and further reading:

Resources, Tools & Solutions:

- [Information Notice Tool](#) created by Cyberwatching.eu.
- [Self assessment checklist for GDPR Readiness Checklist Tool on legal basis](#) (click on "transparency requirements") by the Irish Data Protection Commission.

Further reading:

- [Guidelines on Transparency under Regulation](#) 2016/679, by Article 29 Working Party, as last Revised and Adopted on 11 April 2018.

Q5. Where needed (see [Article 6 GDPR](#)), does your organisation collect individuals consent prior to processing their personal data?

If an SME responded with a positive answer to this question **zero points** would be added to their "GDPR Temperature".

According to the GDPR, where no other lawful bases may apply to the processing of personal data, **prior consent** is necessary in order for the processing to take place legally.

Relying on consent as a legal basis does not automatically mean that consent is valid. In order to ensure that you comply with the criteria stipulated by the GDPR on consent you must ensure that a) consent has been **collected correctly**, and b) that as a controller you are able to **demonstrate** that the data subject has consented to the processing, which may mean that you should have systems in place to collect and store the preferences for consent of the data subject. This evidence may be as simple as a screenshot of the date and time which consent was received or having a database that is regularly updated with all the latest customer preferences.

¹⁸⁶ Art. 14 (2(f)) GDPR.

¹⁸⁷ Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679, as last Revised and Adopted on 11 April 2018, p.6-13.

In addition, **please check the manner** with which the request for consent has been presented, collected, and granted in order to ensure valid consent. Specifically, consent must be:

1. **Freely given:** implying that a real choice and control of the data subjects exists, therefore as a controller you must ensure that this freedom is communicated and able to be exercised by the data subject. For controllers who are **the employers** of data subjects **pay attention** into the inevitable imbalance that exists, therefore not truly allowing the data subject to freely give his consent; thus, before relying on it, assess whether another legal basis can be utilised instead (i.e., the performance of a contract or legal obligation). Attention should also be paid for the cases where the processing operations may involve more than one purpose, in which case the data subjects should be free to choose which purpose they accept rather than having to consent to a bundle or processing purposes.¹⁸⁸ Lastly, it shall be as easy to give consent as it should be to withdraw it.¹⁸⁹
2. **Specific:** reiterating that consent must be given in relation to one or more specific purposes. Having that said, consent may still cover different processing activities (or operations), as long as these operations serve the same purpose. An example of this would include having a separate opt-in for each purpose (for example, marketing and profiling), to allow users to give specific consent for each unique purpose.¹⁹⁰
3. **Informed:** the requirement of transparency is fundamental, especially when relating to consent, because obtaining the relevant information is necessary in order to enable your data subjects to make informed decisions, understand what they are agreeing to, and what rights they may exercise. An example of informed consent is the inclusion of a summary of the privacy policy or at least a mention of the relevant consequences that will apply once the consent is given **and a link to the full privacy policy**. In addition, you must inform the data subject of the right to withdraw consent prior to giving consent.¹⁹¹
4. **Unambiguous:** consisting of a statement from the data subject or a clear affirmative act, through an obvious active motion or declaration. As a data controller, you should be able to show that the consent was indeed granted in a clear way, either via a written or a recorded oral statement – **without the use of pre-ticked opt-in boxes**, which is invalid under the GDPR. Please keep in mind that consent cannot be obtained by the same motion as agreeing to a contract or accepting general terms and conditions of a service. An example of unambiguous consent can be a privacy policy, accompanied by the request for consent through an optional box at the end – which the data subject can actively tick on “I consent.”¹⁹²

In addition, it is crucial that **two additional conditions are met** in order to successfully obtain valid consent: a) **demonstrating that consent has been obtained**, b) ensuring the **withdrawal of consent** is as easy as its granting. In order to demonstrate consent, you should be cautious so as to not obtain more personal data than what is necessary. You should aim to find a way to link the processing activity with the consent given by the data subject, for example you may:

- Keep a record of consent statements received to show how consent was obtained, when it was obtained, the information provided to the data subject at the time of giving consent;
- Sustain a database that is regularly updated with all the latest customer preferences;
- Take a screenshot of the date and time which consent was received;
- In an online environment, retain information on the session in which consent was express, with documentation of the consent workflow at the time of session and a copy of the information that was presented to the data subject at that time.

¹⁸⁸ Guidelines on Consent, p.10.

¹⁸⁹ Art. 7 (3) the General Data Protection Regulation.

¹⁹⁰ Guidelines on Consent, p.11.

¹⁹¹ Guidelines on Consent, p.24.

¹⁹² Guidelines on Consent, p.15.

As pointed out by the European Data Protection Board, “it would not be sufficient to merely refer to a correct configuration of the respective website.”¹⁹³ Furthermore, you should assess for how long consent can last in the specific circumstances of the processing activity (the context, the scope of the original consent and the reasonable expectations of the data subject). If the processing activities change or evolve considerably the original consent will no longer be valid and new consent will need to be obtained. The EDPB recommends refreshing consent at appropriate intervals, depending on the four points mentioned above.

Furthermore, ensuring that withdrawal of consent is a prominent aspect of compliance with guidelines on consent.¹⁹⁴ For example, if consent was obtained through electronic measures (e.g., one mouse-click, swipe, or keystroke) the data subject should in practice be able to withdraw his / her consent in an equally easy manner. If consent was obtained through the use of a service-specific user interface (for example, a website, an app, a browser extension, a log-on account, the interface of an IoT device, or by e-mail, the EDPB expects that the data subject must be able to withdraw consent through the same electronic interface. Switching interfaces between the two phases of collection and withdrawal is considered disproportionate effort and would not be compliant with the EDPB’s guidelines on valid consent. Please keep in mind that, **if the withdrawal right does not meet the above GDPR requirements, the consent mechanism does not comply with the GDPR**. Finally, if the consent is withdrawn the data controller must delete the data that was processed on the basis of consent if no other purpose justifies the continued retention. However, if you chose to **switch from consent to another lawful basis**, you cannot silently migrate from consent to another lawful basis; you must notify the data subject in accordance with Articles 13 and 14.

Additional useful resources, tools and further reading:

Resources, Tools & Solutions:

- [Lawful basis interactive tool](#) produced by the Information Commissioner’s Office (ICO). It is a **useful interactive tool to receive tailored guidance on which lawful basis is likely to be the most appropriate for your processing activities**. This tool will result to a rating for each lawful basis based on the answers to key questions, accompanied by suggestions on the actions you should take.
- [Self assessment checklist for GDPR Readiness Checklist Tool on legal basis](#) (click on “personal data”) by the Irish Data Protection Commission.
- [Clym](#). It is a platform provided by an SME in the United Kingdom and it aims at **website compliance**. It covers 6 main areas of compliance, namely: **Data consent management, Cookie consent management, Localisation and Consent receipts**. This platform can help you keep track of consent receipts, as well as manage cookie consents in an appropriate and transparent manner. The Clym platform can be easily integrated into all major platforms for web design and development.

Further reading:

- [Guidelines 05/2020 on Consent](#) under Regulation 2016/679 Version 1.1, Adopted May 2020.

[Article 29 Working Party Guidelines on consent](#) under Regulation 2016/679, Adopted on November 2017 as last Revised and Adopted on 10 April 2018

Alternatively, if an SME responded with a negative answer to this question, the below recommendation would follow, and **two points would be added** to their “GDPR Temperature”.

According to the GDPR, where no other lawful bases may apply to the processing of personal data, **prior consent** is necessary in order for the processing to take place legally.

¹⁹³ Guidelines on Consent, p.23.

¹⁹⁴ Guidelines on Consent, p.23.

Under the GDPR consent has a two-fold criteria, the act of a **correct collection** of consent, but also the controller's ability to **demonstrate** that the data subject has consented to the processing; therefore, as an SME you must ensure to have systems in place that collect and store the preferences for consent of the data subject.

Additionally, the manner with which the request for consent shall be presented, collected, and granted is important in order to ensure a valid consent. Specifically, consent must be:

- **Freely given:** implying that a real choice and control of the data subjects exists, therefore as a controller you must ensure that this freedom is communicated and able to be exercised by the data subject. For controllers who are **the employers** of data subjects **pay attention** into the inevitable imbalance that exists, therefore not truly allowing the data subject to freely give his consent; thus, before relying on it, assess whether another legal basis can be utilised instead (i.e., the performance of a contract or legal obligation). Attention should also be paid for the cases where the processing operations may involve more than one purpose, in which case the data subjects should be free to choose which purpose they accept rather than having to consent to a bundle or processing purposes.¹⁹⁵ Lastly, it shall be as easy to give consent as it should be to withdraw it.¹⁹⁶
- **Specific:** reiterating that consent must be given in relation to one or more specific purposes. Having that said, consent may still cover different processing activities (or operations), as long as these operations serve the same purpose. An example of this would include having a separate opt-in for each purpose (for example, marketing and profiling), to allow users to give specific consent for each unique purpose.¹⁹⁷
- **Informed:** the requirement of transparency is fundamental, especially when relating to consent, because obtaining the relevant information is necessary in order to enable your data subjects to make informed decisions, understand what they are agreeing to, and what rights they may exercise. An example of informed consent is the inclusion of a summary of the privacy policy or at least a mention of the relevant consequences that will apply once the consent is given **and a link to the full privacy policy**. In addition, you must inform the data subject of the right to withdraw consent prior to giving consent.¹⁹⁸
- **Unambiguous:** consisting of a statement from the data subject or a clear affirmative act, through an obvious active motion or declaration. As a data controller, you should be able to show that the consent was indeed granted in a clear way, either via a written or a recorded oral statement – **without the use of pre-ticked opt-in boxes**, which is invalid under the GDPR. Please keep in mind that consent cannot be obtained by the same motion as agreeing to a contract or accepting general terms and conditions of a service. An example of unambiguous consent can be a privacy policy, accompanied by the request for consent through an optional box at the end – which the data subject can actively tick on “I consent.”¹⁹⁹

In addition, it is crucial that **two additional conditions are met** in order to successfully obtain valid consent: a) **demonstrating that consent has been obtained**, b) ensuring the **withdrawal of consent** is as easy as its granting. In order to demonstrate consent, you should be cautious so as to not obtain more personal data than what is necessary. You should aim to find a way to link the processing activity with the consent given by the data subject, for example you may:

- Keep a record of consent statements received to show: how consent was obtained, when it was obtained, the information provided to the data subject at the time of giving consent;
- Sustain a database that is regularly updated with all the latest customer preferences;
- Take a screenshot of the date and time which consent was received;

¹⁹⁵ Guidelines on Consent, p.10.

¹⁹⁶ Art. 7 (3) the General Data Protection Regulation.

¹⁹⁷ Guidelines on Consent, p.11.

¹⁹⁸ Guidelines on Consent, p.24.

¹⁹⁹ Guidelines on Consent, p.15.

- In an online environment, retain information on the session in which consent was express, with documentation of the consent workflow at the time of session and a copy of the information that was presented to the data subject at that time.

As pointed out by the European Data Protection Board, “it would not be sufficient to merely refer to a correct configuration of the respective website.”²⁰⁰ Furthermore, you should assess for how long consent can last in the specific circumstances of the processing activity (the context, the scope of the original consent and the reasonable expectations of the data subject). If the processing activities change or evolve considerably the original consent will no longer be valid and new consent will need to be obtained. The EDPB recommends to refresh consent at appropriate intervals, depending on the four points mentioned above.

Furthermore, ensuring that withdrawal of consent is a prominent aspect of compliance with guidelines on consent.²⁰¹ For example, if consent was obtained through electronic measures (e.g., one mouse-click, swipe, or keystroke) the data subject should in practice be able to withdraw his / her consent in an equally easy manner. If consent was obtained through the use of a service-specific user interface (for example, a website, an app, a browser extension, a log-on account, the interface of an IoT device, or by e-mail, the EDPB expects that the data subject must be able to withdraw consent through the same electronic interface. Switching interfaces between the two phases of collection and withdrawal is considered disproportionate effort and would not be compliant with the EDPB’s guidelines on valid consent. Please keep in mind that, **if the withdrawal right does not meet the above GDPR requirements, the consent mechanism does not comply with the GDPR**. Finally, if the consent is withdrawn the data controller must delete the data that was processed on the basis of consent if no other purpose justifies the continued retention. However, if you chose to **switch from consent to another lawful basis**, you cannot silently migrate from consent to another lawful basis; you must notify the data subject in accordance with Articles 13 and 14.

As a last note and as can be concluded from the above, consent is not an easy legal basis to implement, and it brings upon many further requirements that can burden an SME. Consent may not always be the right legal basis, therefore, before counting on consent and creating systems to ensure that it is valid, you should first check:

- Is the processing necessary for the **performance of a contract** or to take steps **at the request of the data subject** prior to entering into a contract? (Art. 6 (1) (b) GDPR)
- Is the processing necessary for your compliance with a **legal obligation** to which you are subject to? (Art. 6 (1) (c) GDPR)
- Is the processing necessary for the **protection of vital interests** of the data subject or another natural person? (Art. 6 (1) (d) GDPR)
- Is the processing necessary for the performance of a task carried out in the **public interest** or in the exercise of **official authority vested in you**? (Art. 6 (1) (e) GDPR)
- Is the processing necessary for the purposes of the **legitimate interest** pursued by you or a third party? (Art. 6 (1) (f) GDPR)

If any of the above legal basis applies, then the legal basis of consent is not necessary and should be avoided.

Not implementing a valid consent into the processing activities is a serious risk, because it means that your company is processing personal data without a lawful basis. Under the GDPR, violations on such basic principles of processing may result to administrative fines up to 20 000 000 EUR, or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.²⁰² Additionally, some European Member States may also provide for additional sanctions (such as criminal sanctions).²⁰³

²⁰⁰ Guidelines on Consent, p.23.

²⁰¹ Guidelines on Consent, p.23.

²⁰² Art. 83 (5(a)) GDPR.

²⁰³ Artt. 83 (9) and 84 GDPR.

Additional useful resources, tools and further reading:**Resources, Tools & Solutions:**

- [Lawful basis interactive tool](#) produced by the Information Commissioner's Office (ICO). It is a **useful interactive tool to receive tailored guidance on which lawful basis is likely to be the most appropriate for your processing activities**. This tool will result to a rating for each lawful basis based on the answers to key questions, accompanied by suggestions on the actions you should take.
- [Self assessment checklist for GDPR Readiness Checklist Tool on legal basis](#) (click on "personal data") by the Irish Data Protection Commission.
- [Clym](#). It is a platform provided by an SME in the United Kingdom and it aims at **website compliance**. It covers 6 main areas of compliance, namely: **Data consent management, Cookie consent management, Localisation and Consent receipts**. This platform can help you keep track of consent receipts, as well as manage cookie consents in an appropriate and transparent manner. The Clym platform can be easily integrated into all major platforms for web design and development.
- The [DEFEND project](#) supports **healthcare** organizations towards GDPR compliance and it provides methods and automation techniques for the specification, management and enforcement of personal data consent; a modular solution that covers different aspects of GDPR.

Further reading:

- [Guidelines 05/2020 on Consent](#) under Regulation 2016/679 Version 1.1, Adopted May 2020.
- [Article 29 Working Party Guidelines on consent](#) under Regulation 2016/679, Adopted on November 2017 as last Revised and Adopted on 10 April 2018.

Q6. Does your organisation allow for data subjects to exercise their data subject rights?

If an SME responded with a positive answer to this question **two points would be deducted** from their "GDPR Temperature".

The GDPR obliges controllers to provide data subjects with relevant information as to the existence of their rights, and how they can be exercised (Arts. [13\(2\)\(b\)](#) and [14\(2\)\(c\) GDPR](#)). This means that your organisation must also develop a consistent and effective approach to receiving, tracking and addressing any requests received from data subjects to exercise any of the data subject rights.

Please ensure that you **trace all requests** received and responses given to those requests, in order to ensure that you respond and address the data subject request in a timely manner (within one month of the receipt). You can demonstrate compliance with the GDPR rules by following the good practice of **keeping a register of data subject requests**, listing:

- the dates on which a request was received and resolved,
- the identity of the requester,
- the scope of the request, and
- storing evidence of the actual communications exchanged with requesters.

The principle of transparency places a triple obligation upon the controller concerning the rights of data subjects, 1) provide information to data subjects on their rights (as required under Articles 13 (2)(b) and 14 (2)(c) GDPR, 2) comply with the principle of transparency when communicating with data subjects in relation to their rights under Articles 15 to 22 and Article 34 GDPR, 3) facilitate the exercise of data subjects' rights.²⁰⁴

Additional useful resources, tools and further reading:

²⁰⁴ Article 29 Working Party Guidelines on transparency under Regulation 2016/679 Adopted on November 2017, as last revised and adopted on April 2018, p.26.

Resources, Tools & Solutions:

- A template for the [Right to Erasure Request Form](#) is provided by the [gdpr.eu](#) project, a project funded by the European Union Horizon 2020 can be relied on to create a workflow and have a template for handling the right to erasure, which is one of the more complication rights to be exercised per the GDPR.
- [Self assessment checklist for GDPR Readiness Checklist Tool on legal basis](#) (click on “data subject rights”) by the Irish Data Protection Commission.

Further reading:

- Further [guidance on the right of access](#) has been provided by the Information Commissioner’s Office (ICO).
- [Step-by-step Guide on how to deal with a request for information](#) by the ICO.
- [Frequently Asked Questions on the Data Subject Access Requests](#) by the Irish Data Protection Commission.

If an SME responded with a negative answer to this question, the below recommendation would follow and **two points would be added** to their “GDPR Temperature”.

The GDPR obliges controllers to provide data subjects with relevant information as to the existence of their rights, and how they can be exercised (Arts. [13\(2\)\(b\)](#) and [14\(2\)\(c\)](#) GDPR). This means that your organisation must also develop a consistent and effective approach to receiving, tracking and addressing any requests received from data subjects to exercise any of the rights described below.

The approach which a controller chooses to implement regarding the response to data subject rights must consider several factors in order to correctly manage those responses under the GDPR, regardless of the type of request which is made. Once you receive a request, you must first take steps to **reasonably identify and authenticate the requester**, depending on the scope of the request and the level of risk involved. Having confirmed the identity of the requester, the controller should also confirm whether the organisation handles any personal data related to the requester. If not, the controller will be unable to address the request made, and should notify the requester of this. On the other hand, if it is confirmed that personal data related to the requester is processed by the controller, then it will be important to **identify the type of request made**, in order to properly respond. As a rule, all requests should be handled free of charge, unless the request is considered unfounded or excessive (for example, if the requester has made a similar or the same one in the past, or where the scope of a request is excessively broad), may the controller refuse to act on that request or charge a reasonable amount in order to respond ([Art. 12\(5\) GDPR](#)). Please ensure that you respond and address the data subject request in a timely manner, at most within one month of receipt of the request.

The principle of transparency places a triple obligation upon the controller concerning the rights of data subjects, 1) provide information to data subjects on their rights (as required under Articles 13 (2)(b) and 14 (2)(c)) GDPR, 2) comply with the principle of transparency when communicating with data subjects in relation to their rights under Articles 15 to 22 and Article 34 GDPR, 3) facilitate the exercise of data subjects’ rights.²⁰⁵

As mentioned above, the controller must keep track of all requests received and responses given to those requests, so that it can demonstrate its compliance with the GDPR rules, therefore it is good practice to **keep a register of data subject requests**, listing:

- the dates on which a request was received and resolved,
- the identity of the requester,
- the scope of the request, and

²⁰⁵ Article 29 Working Party Guidelines on transparency under Regulation 2016/679 Adopted on November 2017, as last revised and adopted on April 2018, p.26.

- storing evidence of the actual communications exchanged with requesters.

Below are the rights that you must inform a data subject of, and ensure that they are able to exercise them easily:

- 1) The right of access to a) obtain confirmation from the controller as to whether or not personal data concerning him/her are being processed; b) those personal data and receive a copy of those personal data, c) receive information about the processing of personal data undertaken.
- 2) The right to rectification allows the data subject to indicate the information which he/she wishes to correct or complete,
- 3) The right to erasure, or 'right to be forgotten' (Art. 17 GDPR) needs to have a specific scope in order for the request for erasure to be considered valid. Data subjects are allowed to demand that a controller erase personal data relating to them if:
 - those data are no longer necessary in relation to the purposes for which they were collected or are processed by the controller (Art. 17(1)(a) GDPR);
 - the personal data were processed on the basis of the data subject's consent, and the data subject withdrew the consent given;
 - the data subject files a valid objection to the processing of their personal data by the controller (more on the right to objection below);
 - the personal data have been processed unlawfully;
 - an applicable legal obligation upon the controller, rooted in EU or Member State law, requires the controller to erase those personal data; or
 - the personal data were collected in the context of the provision of information society services to children, on the basis of consent provided by those children or adults with parental responsibilities over those children (Art. 8 GDPR).

The gdpr.eu project is a project funded by the European Union Horizon 2020 and provides many useful resources for organisations and individuals researching the General Data Protection Regulation. It provides information to help organisations achieve GDPR compliance, including different templates, such as the template for the [Right to Erasure Request Form](#). You can rely on this template in order to create a workflow and have a template for handling the right to erasure, which is one of the more complication rights to be exercised per the GDPR.

- 4) The right to restriction of processing allows data subjects to request that controllers place their personal data under restricted conditions of use. However, it is important to note that as set out in Art. 18 (2) GDPR, the controller can continue to store personal data covered by a request for restriction of processing. In addition, in order for such a request to be valid the data subject must either have a) contested the accuracy of the personal data processed (Art. 18 (1(a)) GDPR), the processing must be unlawful (Art. 18(1(b)) GDPR), the controller no longer requires the personal data in connection to the purposes for their collection and processing (Art. 18(1(c)) GDPR), or the data subject has objected to the processing of personal data and the controller requires time to assess whether to grant the objection or not (Art. 18(1(d)) GDPR).
- 5) The right to data portability (Art. 20 GDPR) gives individuals the right to receive personal data they have provided to the controller in a structured, commonly used and machine-readable format. In addition, it includes the right to request that a controller transmit those data directly to another controller.²⁰⁶ The data subject should not have any hindrance in exercising this right, whether it be legal, technical,

²⁰⁶ Guidelines on the right to "data portability", Adopted on 13 December 2016, as last Revised and adopted on 5 April 2017, pages 15-16.

or financial obstacles which may refrain or slow down access, transmission, reuse by the data subject (for example, requesting a fee, lack of interoperability format or access to a data format / API, excessive delays in retrieving the full dataset, etc.).²⁰⁷ Data controllers could evaluate two different ways of providing portable data to the data subjects or to other data controllers: a) a direct transmission of the overall dataset of portable data (or several extracts of parts of the global dataset); b) an automated tool that allows extraction of relevant data.

- 6) The right to object to processing (Art. 21 GDPR) allows data subjects to seek to prevent a controller from continuing to process their personal data for a given purpose, such as the right to object to the processing of their personal data for direct marketing purposes (Art. 21(2) GDPR), including profiling activities.
- 7) The rights concerning automated individual decision-making (Art. 22 GDPR) which include a set of rights for data subjects in relation to processing activities that classify as 'automated individual decision-making'. If you carry out processing activities that rely on automated individual decision-making, please respond to question 7 and carefully study the recommendations provided.

Additional useful resources, tools and further reading:

Resources, Tools & Solutions:

- A template for the [Right to Erasure Request Form](#) is provided by the [gdpr.eu](#) project, a project funded by the European Union Horizon 2020 can be relied on to create a workflow and have a template for handling the right to erasure, which is one of the more complication rights to be exercised per the GDPR.
- [Self assessment checklist for GDPR Readiness Checklist Tool on legal basis](#) (click on "data subject rights") by the Irish Data Protection Commission.

Further reading:

- Further [guidance on the right of access](#) has been provided by the Information Commissioner's Office (ICO).
- [Step-by-step Guide on how to deal with a request for information](#) by the ICO.
- [Frequently Asked Questions on the Data Subject Access Requests](#) by the Irish Data Protection Commission.
- [Guidelines on the right to "data portability"](#), Adopted on 13 December 2016, as last revised and adopted on 5 April 2017, by the Article 29 Working Party.

Q7. Does your organisation offer online services directly to children aged 13 or over?

If an SME responded with a positive answer to this question, the below recommendation would follow and **two points would be added** to their "GDPR Temperature".

Children, due to their nature and lack of maturity may be less aware of the risks, consequences and security when it comes to providing and protecting their personal data online, therefore a company that offers services to children should be aware that they are taking a greater risk and should introduce even more specific and enhanced safeguards. The GDPR creates an additional layer of protection for all types of collection of personal data of children regardless of its nature. Keep in mind that the age consideration to define "children" is where the child is at least 16 years old, however, the GDPR leaves leeway for each European Member State to decide whether to lower the age to the minimum of 13 years old or somewhere in between."²⁰⁸

Additional useful resources, tools and further reading:

Further reading:

- [Children's Code hub](#) is a set of resources that has been collated by the Information Commissioner's Office (ICO).
- [Age appropriate design: Code of practice for online services](#) is a data protection code of practice for online services, such as apps, online games, and web and social

²⁰⁷ Guidelines on the right to "data portability", Adopted on 13 December 2016, as last Revised and adopted on 5 April 2017, pages 15-16.

²⁰⁸ Art. 8 (2) GDPR.

media sites, likely to be accessed by children, created by ICO. This Code aims to set a benchmark for the appropriate protection of childrens' personal data and asks for controllers to build the standard into the design processes, upgrades and services' development processes. It also includes a reference to a [Data Processing Impact Assessment](#) which can be used to record the process and result of the impact of an online service likely to be accessed by children.

- [Children's Fundamentals](#) – A guide to protecting children's personal data published by the Irish Data Protection Commission (DPC)
- [The rights of children and young people on digital platforms](#) has been created by the Swedish Authority for Privacy Protection and provides general support on data protection regulation for children.

If an SME responded with a negative answer to this question **zero points** would be added to their "GDPR Temperature".

If the answer to question 7) is yes:

Q7B. Does your organisation collect the consent from the parent or from someone holding the parental responsibility for the child?

If an SME responded with a positive answer to this question, the below recommendation would be proposed, and **zero points** would be added to their "GDPR Temperature".

If an SME responded with a negative answer to this question, then the below recommendation would pop up and **two points** would be added to their "GDPR Temperature".

Where the child is below the age of 16 years, or a lower age provided by each Member State law, the processing of the personal data of a child being offered information society services is only lawful if **the consent is given or authorised by the holder of parental responsibility** over the child.²⁰⁹ Therefore, it is clear that receiving valid consent from parents is a crucial point when it comes to handling the personal data of children. If your company offers information society services directly to children, not having a procedure to **collect parental consent** will highly raise the risks to be sanctioned under the GDPR.

In order to ensure that consent is obtained, where necessary, you will need to establish the age of the child with a level of certainty. The ICO has produced a Code of practice for age-appropriate design for online services which would ensure that the methods used is appropriate to the risks that arise from your data processing. Some methods to establish the age of the child include²¹⁰:

- **Self-declaration** – Where a user simply states their age but does not provide any evidence to confirm it. It may be suitable for low-risk processing or when used in conjunction with other techniques. Even if you prefer to apply the standards in the code to all your users, self-declaration of age can provide a useful starting point when providing privacy information and age-appropriate explanations of processing.
- **Artificial intelligence** – It may be possible to make an estimate of a user's age by using artificial intelligence to analyse the way in which the user interacts with your service. Similarly, you could use this type of profiling to check that the way a user interacts with your service is consistent with their self-declared age. This technique will typically provide a greater level of certainty about the age of users with increased use of your service. If you choose to use this technique then you need to: i. tell users that you are going to do this upfront; ii. only collect the minimum amount of personal data that you need for this purpose; and iii. not use any personal data you collect for this purpose for other purposes.
- **Third party age verification services** – You may choose to use a third-party service to provide you with an assurance of the age of your users. Such services typically work on an 'attribute' system where you request confirmation of a particular user attribute (in this case age or age range) and the service provides you with a 'yes' or 'no' answer. This method reduces the amount of personal data you need to collect yourself and may allow you to take advantage of technological expertise and

²⁰⁹ Guidelines on Consent, p.24.

²¹⁰ Age appropriate design: code of practice for online services, available [here](#).

latest developments in the field. If you use a third-party service you will need to carry out some due diligence checks to ensure that the level of certainty with which it confirms age is sufficient (PAS standard 1296 'Online age checking' may help you with this), and that it is compliant with data protection requirements. You should also provide your users with clear information about the service you use.

- **Account holder confirmation** - You may be able to rely upon confirmation of user age from an existing account holder who you know to be an adult. For example, if you provide a logged-in or subscription-based service, you may allow the main (confirmed adult) account holder to set up child profiles, restrict further access with a password or PIN, or simply confirm the age range of additional account users.
- **Technical measures** – Technical measures which discourage false declarations of age, or identify and close underage accounts, may be useful to support or strengthen self-declaration mechanisms. Examples include neutral presentation of age declaration screens (rather than nudging towards the selection of certain ages), or preventing users from immediately resubmitting a new age if they are denied access to your service when they first self-declare their age.
- **Hard identifiers** – You can confirm age using solutions which link back to formal identify documents or 'hard identifiers' such as a passport. However, we recommend that you avoid giving users only the choice of providing hard identifiers, unless the risks inherent in your processing really warrant such an approach. Some children do not have access to formal identity documents and may have limited parental support, making it difficult for them to access age verified services at all, even if they are age appropriate. Requiring hard identifiers may also have a disproportionate impact on the privacy of adults.

The administrative fines applicable in cases of violations to a data controller's obligation to receive valid consent for processing children's personal data may be up to 10 000 000 EUR or up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Additional useful resources, tools and further reading:

Further reading:

- [Guidelines 05/2020 on Consent](#) under Regulation 2016/679 Version 1.1, Adopted May 2020, pages 25-29.
- [Age appropriate design](#): code of practice for online services.
- [Guide on consent](#) published by the Information Commissioner's Office (ICO).

Q8. Does your organisation put in place any form of automated processing of personal data that involves the use of personal data to evaluate certain personal aspects relating to a natural person, such as to analyse or predict its personal preferences, interests, behaviour, etc. (i.e., profiling)?

If an SME responded with a positive answer to this question, then the below recommendation would pop up and **four points** would be **added** to their "GDPR Temperature".

Initially, the GDPR stipulates that the data subject shall have the right **not to be subject** to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.²¹¹ Therefore, if you plan to conduct any automated individual decision-making (that produces legal effects to the data subject), the only way to do so is if the decision:

- is necessary for entering into, or performance of, a contract between the data subject and a data controller; or
- is authorised by European or Member State law to which the controller is subject to and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

²¹¹ Art. 22 (1) GDPR.

- is based on the data subject's explicit consent.²¹²

If one of the above legitimate basis is used, as a controller, you must still implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, including at least the right to obtain human intervention, to express his or her point of view, and to contest the decision (made through automated processing).²¹³ In short, this means that if you implement automated individual-decision making, the European legislators expect further rights to be available to data subjects.

Please keep in mind that automated decision-making that involves special categories of personal data is **only** allowed if the controller has received **explicit consent** from the data subject, or if there is a **substantial public interest** to conduct such decision making. Naturally, the safeguards implemented (and mentioned later) must be more suitable, and of a higher level.²¹⁴

So, what exactly are the elements to assess whether you are conducting automated decision-making? Overall, a decision based solely on automated processing means that there is **no human involvement** in the decision process.

However, pay attention to the fact that even if there is a routinely human involvement, but it does not actually influence the result of the automatic decision making, this can still be considered a decision based solely on automated processing. In short, if you are unsure of whether your processing qualifies as an automated processing, then, we recommend assessing whether any human involvement has a meaningful oversight, such as someone who has authority to change the decision, rather than a mere formality. For example, if a tool is implemented on roads in order to verify the speed limit of cars and marks them as above the speed limit, the decision of imposing a speeding fine will be solely based on automated decision making. Continuing with this scenario, if a policeman is involved merely to notify the speeding fines to the car driver and does not have the power to influence the decision itself, this **cannot be** considered human intervention for the purpose of Article 22.

Further, a decision based solely on automated processing needs to produce 'legal' or 'similarly significant effects', meaning that the decision must include serious impactful effects for a data subject, in order for it to be covered under this definition.²¹⁵ On the one side, examples of this type of 'legal' effect may be something that affects a person's legal status, or their rights under a contract, such as the termination of a contract, the entitlement / denial of a social benefit granted by law, etc. On the other side, other 'similarly significant effects' may also be sufficient to trigger the definition of automated decision-making, so long as such effects significantly affect the circumstances, behaviour or choices of the individuals concerned, and have a prolonged or permanent impact on the data subject. Examples of decisions that have 'similarly significant effects' may include intrusive profiling, automatic refusal of an online credit application, e-recruiting practices without any human intervention, or decisions that affect someone's access to health services, or to education (i.e., university admissions).²¹⁶

Automated decision-making may partially overlap with profiling; since online advertising has increased reliance on automated tools. In many typical cases, the decision to present targeted advertising based on profiling will not have similarly significant effects on individuals (for example, an advertisement for an online shop based on simple demographic profile 'woman, in Italy, aged between 20 and 30'). However, it is possible that profiling falls under the definition of automated decision-making if the particular case a) implies **intrusive profiling process** (i.e., tracking individuals across different websites, devices and services), or b) includes an **obvious advert delivery**, using knowledge of the vulnerabilities of the data

²¹² Art. 22 (2) GDPR.

²¹³ Art. 22 (3) GDPR.

²¹⁴ Art. 22 (4) GDPR.

²¹⁵ Guidelines on Automated individual decision-making and profiling, for the purposes of Regulation 2016/679, pg. 21.

²¹⁶ Guidelines on Automated individual decision-making and profiling, for the purposes of Regulation 2016/679, pg. 22.

subjects targeted. Additionally, differential pricing based on profiling characteristics and behaviours of the user may also have ‘significant effects’, if that person is essentially limited from buying certain goods or services. Please note that if the profiling relates to social media profiling and / or targeting (such as by a social media provider) is likely to have a “similarly significant effect on a data subject”, Article 22 will be applicable. The EDPB highlights that this means the **controller must**, in each instance of targeting, **conduct a case-by-case assessment to decide whether the profiling will similarly significantly affect** a data subject with reference to the specific facts of the targeting.²¹⁷ Therefore, automated decision-making may partially overlap with or result from profiling. If you assess that the online social media targeting you are carrying out falls within the scope of Article 22 (meaning that targeting would have the potential to significantly and adversely affect a data subject), then one of the legal basis outlined above would be required.²¹⁸

All in all, where the decision stemming from profiling activity is **solely** based on automated decision-making, and it produces legal effects, or similarly significant effects, then the profiling is also an automated decision-making processing.

As a controller, you may carry out profiling and automated decision-making so long as you respect all the principles and have a proper legal basis for the processing. A key accountability tool is the Data Protection Impact Assessment, since automated decision-making activities may often lead to high risks for the data subjects. Carrying out a DPIA will both enable you to assess the risks of the processing activity, as well as demonstrate that you have put in place appropriate measures to address those risks.²¹⁹ Furthermore, Article 35(3) GDPR describes that a processing activity likely to result in high risks includes a systematic and extensive evaluation of personal aspects which is based on automated decision-making, including profiling. Therefore it is highly recommended that you carry out a DPIA, but if you decide not to, please check whether automated decision-making and profiling fall within the activities that must mandatorily carry out a DPIA, which are available [here](#) but also in the designated national supervisory authority’s website.

In addition, when it comes to solely automated decision-making, including profiling, you must apply additional safeguards for all the general principles of the GDPR, such as:

- while providing data protection related information to the data subject (i.e., in the privacy policy), you must additionally provide meaningful information about the logic involved in the automated decision making, as well as the significance and envisaged consequences of such processing for data subjects, for example, how the automated decision-making process is built and how it is used for a decision concerning the data subject;²²⁰
- providing the right to object to the automated processing has to be explicitly mentioned to the data subject, presented clearly and separately from other information.²²¹

Automated processing of personal data allows you to have a structured understanding of your data subjects that may be exploited in several ways, therefore the GDPR requires that automated processing should be accompanied by appropriate safeguards. Below you can find a list drafted by the European Data Protection Board (also known as Working Party 29), which has attempted to offer some good practice recommendations for controllers’ safeguards²²²:

- quality checks of systems, regularly, to ensure that individuals are treated fairly;
- algorithmic auditing, by testing the algorithms used and developed by machine learning systems, to check their performance;

²¹⁷ [Guidelines 8/2020 on the targeting of social media users](#), Version 2.0, Adopted on 13 April 2021, pg.25.

²¹⁸ [Guidelines 8/2020 on the targeting of social media users](#), Version 2.0, Adopted on 13 April 2021, pg.26.

²¹⁹ Guidelines on Automated individual decision-making and profiling, for the purposes of Regulation 2016/679, pg. 29.

²²⁰ Art. 13 (2) (f) GDPR.

²²¹ Art. 21 (4) GDPR.

²²² Guidelines on Automated individual decision-making and profiling, for the purposes of Regulation 2016/679, pg. 32.

- incorporating data minimisation in the automated processes, by identifying clear retention periods for profiles and any other personal data used;
- implementing anonymisation or pseudonymisation techniques in the context of profiling;
- the creation of a mechanism where data subjects can request human intervention when they are affected by a decision that is solely based on automated processing (i.e., providing an appeal process). For example, if you receive an e-mail that informs you of an automated decision made using your personal data, in the footer of this e-mail it should be notified that this decision was taken in this way, and also offering a link usable to request a human intervention to be involved in this decision.

Additional useful resources, tools and further reading:

Further reading:

- Guidelines on Automated individual decision-making and profiling, for the purposes of Regulation 2016/679.

If an SME responded with a negative answer to this question, then **zero points** would be added to their "GDPR Temperature".

If you plan to conduct any automated individual decision-making (that produces legal effects to the data subject), the only way to do so is if the decision:

- is necessary for entering into, or performance of, a contract between the data subject and a data controller; or
- is authorised by European or Member State law to which the controller is subject to and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- is based on the data subject's explicit consent.²²³

So, what exactly are the elements to assess whether you are conducting automated decision-making? Overall, a decision based solely on automated processing means that there is **no human involvement** in the decision process.

However, if you are unsure of whether your processing qualifies as an automated processing, then, we recommend assessing whether any human involvement has a meaningful oversight, such as someone who has authority to change the decision, rather than a mere formality. For example, if a tool is implemented on roads in order to verify the speed limit of cars and marks them as above the speed limit, the decision of imposing a speeding fine will be solely based on automated decision making. Continuing with this scenario, if a policeman is involved merely to notify the speeding fines to the car driver and does not have the power to influence the decision itself, this **cannot be** considered human intervention for the purpose of Article 22.

Further, a decision based solely on automated processing needs to produce 'legal' or 'similarly significant effects', meaning that the decision must include serious impactful effects for a data subject, in order for it to be covered under this definition.²²⁴ On the one side, examples of this type of 'legal' effect may be something that affects a person's legal status, or their rights under a contract, such as the termination of a contract, the entitlement / denial of a social benefit granted by law, etc. On the other side, other 'similarly significant effects' may also be sufficient to trigger the definition of automated decision-making, so long as such effects significantly affect the circumstances, behaviour or choices of the individuals concerned, and have a prolonged or permanent impact on the data subject. Examples of decisions that have 'similarly significant effects' may include intrusive profiling, automatic refusal of an online credit application, e-recruiting practices without any human intervention,

²²³ Art. 22 (2) GDPR.

²²⁴ Guidelines on Automated individual decision-making and profiling, for the purposes of Regulation 2016/679, pg. 21.

or decisions that affect someone's access to health services, or to education (i.e., university admissions).²²⁵

Automated decision-making may partially overlap with profiling; since online advertising has increased reliance on automated tools. In many typical cases, the decision to present targeted advertising based on profiling will not have similarly significant effects on individuals (for example, an advertisement for an online shop based on simple demographic profile 'woman, in Italy, aged between 20 and 30'). However, it is possible that profiling falls under the definition of automated decision-making if the particular case a) implies **intrusive profiling process** (i.e., tracking individuals across different websites, devices and services), or, b) includes an **obvious advert delivery**, using knowledge of the vulnerabilities of the data subjects targeted. Additionally, differential pricing based on profiling characteristics and behaviours of the user may also have 'significant effects', if that person is essentially limited from buying certain goods or services. Please note that if the profiling relates to social media profiling and / or targeting (such as by a social media provider) is likely to have a "similarly significant effect on a data subject", Article 22 will be applicable. The EDPB highlights that this means the **controller must**, in each instance of targeting, **conduct a case-by-case assessment to decide whether the profiling will similarly significantly affect** a data subject with reference to the specific facts of the targeting.²²⁶ Therefore, automated decision-making may partially overlap with or result from profiling. If you assess that the online social media targeting you are carrying out falls within the scope of Article 22 (meaning that targeting would have the potential to significantly and adversely affect a data subject), then one of the legal basis outlined above would be required.²²⁷

All in all, where the decision stemming from profiling activity is **solely** based on automated decision-making, and it produces legal effects, or similarly significant effects, then the profiling is also an automated decision-making processing.

Additional useful resources, tools and further reading:

Further reading:

- Guidelines on Automated individual decision-making and profiling, for the purposes of Regulation 2016/679.

Q9. Does your organisation transfer data outside the EU?

If an SME responded with a positive answer to this question, then the below recommendation would pop up and **four points** would be added to their "GDPR Temperature".

Any transfers of personal data outside the European Union should always be made with caution, because the GDPR only allows for such transfers under a strict lawfulness mechanism stipulated in the GDPR to ensure that the transfer is subject to appropriate safeguards.

The first step is to identify, as an exporter, the transfers of personal data outside of the EEA and secondly verify the corresponding transfer mechanism that the transfer will be relied on.²²⁸ Knowing your transfers means recording and mapping them, and understanding your processors and sub-processors. A good practice is to build on the records of processing activities (if you are obliged to maintain them) and include the transfers of data. Also map further or onward transfers (for instance whether your processors outside the EEA transfer your personal data to a sub-processor in another third country).²²⁹ Please be aware that

²²⁵ Guidelines on Automated individual decision-making and profiling, for the purposes of Regulation 2016/679, pg. 22.

²²⁶ [Guidelines 8/2020 on the targeting of social media users](#), Version 2.0, Adopted on 13 April 2021, pg.25.

²²⁷ [Guidelines 8/2020 on the targeting of social media users](#), Version 2.0, Adopted on 13 April 2021, pg.26.

²²⁸ [Recommendations 01/2020 on measures that supplement transfer tools](#) to ensure compliance with the EU level of protection of personal data, Adopted on 10 November 2020, European Data Protection Board, pages 8-9.

²²⁹ [Recommendations 01/2020 on measures that supplement transfer tools](#) to ensure compliance with the EU level of protection of personal data, Adopted on 10 November 2020, European Data Protection Board, page 9.

remote access from a third country or cloud storage in a cloud situated outside the EEA is also considered a transfer.²³⁰

The second step is to identify the transfer tools you will rely on. Firstly, check the European Commission's adequacy decisions ([Article 45 GDPR](#)), which at the moment only offer safeguards for a small portion of non-EU countries.²³¹ The existence of an adequacy decision means you're your company can transfer to that country without any specific authorisation or extra safeguards than those implemented for transfers within the European Union. You may find a list of the adequacy decisions [here](#). If you rely on an adequacy decision, you do not need to take into consideration the below safeguards.

However, for the majority of the cases, there is an absence of an adequacy decision, which means that as a controller or processor, you may only transfer personal data if you have provided appropriate safeguards to ensure the availability of rights and legal remedies for data subjects ([Article 46 GDPR](#)). Below are some transfer tools that the GDPR offers to provide such safeguards:

- [Standard data protection clauses adopted by the Commission](#), which are probably the most common way of transferring personal data outside the European and are stipulated in [Article 46 GDPR](#). These clauses are model clauses that give the necessary mandate and ensures that safeguards will be implemented in the transfers. It is the most preferred method of legally transferring personal data to non-EU countries because these model clauses can be attached to any contractual agreement or data protection agreement that is to be signed between the exporter (company sending the personal data) and the importer (company receiving the personal data). The final working document of the Standard Contractual Clauses (SCCs) was published on June 4th 2021, and will enter into force twenty days after the publication in the Official Journal of the European Union. The old version of the Standard Contractual Clauses which have been relied on by companies until 2021 will be **repealed three months after the new SCCs enter into force**. This means that if your company enters into new contracts with non-EU processors after the old SCCs were repealed, you must use the new SCCs. If your company concluded a contract including the **old SCCs prior to the date of their repeal, it will be a valid transfer mechanism for 15 months following the date of their repeal**. In short, approximately within the transition period of 18 months, you must substitute the old SCCs with the new version published in 2021. companies who transfer personal data to non-EU.
- Codes of conduct, which have been approved by the competent supervisory authority (meaning, the supervisory authority that is on the territory of the main establishments of your company). If you comply with a code of conduct, you shall still have binding and enforceable commitments from the controller or processor in the non-EU country, in order to ensure that the appropriate safeguards are applied equally to their operations. In fact, on May 19th 2021 the Belgian Data Protection Authority [approved](#) the first transnational code of conduct adopted within the EU since the GDPR entered into force, namely, the [EU Data Protection Code of Conduct for Cloud Service Providers](#).
- Certification mechanisms, which have been approved by the competent supervisory authority (meaning, the supervisory authority that is on the territory of the main establishments of your company). If you comply with a certification mechanism, you shall still have binding and enforceable commitments from the controller or processor in the non-EU country, in order to ensure that the appropriate safeguards are applied equally to their operations.
- Binding Corporate Rules (also known as "BCRs"), is a transfer mechanism that may not be easily applicable to SMEs since it mostly applies to group of undertakings or enterprises that are engaged in a joint economic activity ([Article 47 GDPR](#)).

²³⁰ [European Data Protection Board Frequently Asked Questions](#) on the judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems, 23 July 2020, FAQ nr. 11.

²³¹ Article 45 (1) General Data Protection Regulation.

However, if this is applicable to you, the Binding Corporate Rules are an internal binding contract for the purpose of ensuring that all data transfers within a corporate group are on an adequate level of protection, and must contain both privacy principles (i.e., transparency, data minimisation, purpose limitation) and tools of effectiveness (i.e., audit, training, or complaint handling systems) of the agreement.

²³² The EDPB also provides a [list of the BCRs](#) approved under the GDPR.

- In the absence of any of the above safeguards for transfers, there are specific derogations that may allow you to continue transferring the personal data to a third country; for example:
 - if the data subject has explicitly consented to the proposed transfer (after having been informed of possible risks), or
 - if the transfer is based on the performance of a contract at the data subject's request, or
 - the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject, or
 - the transfer is necessary for important reasons of public interest, or
 - for the establishment, exercise or defence of legal claims, or
 - if the transfer is necessary to protect the vital interest of the data subject or of other persons, or
 - if the transfer is made from a register which according to Union or Member State law is intended to provide information to the public.²³³

The third step is to assess the circumstances of the transfer and the effectiveness of the transfer tool you chose. Depending on the result of this assessment, it may be necessary to implement additional measures to ensure an equivalent level of protection to that of within the EEA. Therefore, you must assess, with the collaboration of the importer, any aspects of the law or practice in the third country to which you are transferring personal data that hinder the effectiveness of the transfer tool you rely on.²³⁴ This assessment must take into consideration, for example,

- all actors participating in the transfer (controllers, processors, sub-processors processing data in the third country)
- any onward transfers that may occur
- the domestic legal order of the country to which the data is transferred (or onward transferred),
- the applicable legal context will depend on the circumstances of the transfer, in particular:
 - the purposes for which the data are transferred (e.g., marketing, HR, storage, IT support, etc.)
 - types of entities involved in the processing (public/private, controller/processor, etc.)
 - sector in which the transfer occurs (e.g., adtech, telecommunication, financial, etc.)
 - categories of personal data transferred
 - storage in third country or mere remote access to data storage within EU/EEA
 - format of data to be transferred (will it be in plain text, pseudonymised or encrypted?)
 - possibility that the data may be onward transferred.²³⁵

²³² Available on: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en.

²³³ Article 49 General Data Protection Regulation. For more details on the derogations are available on the Guidelines on 2/2018 on derogations of Article 49 under Regulation 2016/679.

²³⁴ [Recommendations 01/2020 on measures that supplement transfer tools](#) to ensure compliance with the EU level of protection of personal data, Adopted on 10 November 2020, European Data Protection Board, page 12.

²³⁵ [Recommendations 01/2020 on measures that supplement transfer tools](#) to ensure compliance with the EU level of protection of personal data, Adopted on 10 November 2020, European Data Protection Board, page 12.

- Assess whether the applicable laws²³⁶:
 - impinge on the commitments to enable data subject rights in the context of international transfers, or in their fundamental rights, especially the right of redress in case of access by third country public authorities to the transferred data;
 - require the disclosure of personal data to public authorities or granting such public authorities powers to access personal data (in the context of criminal law enforcement, regulatory supervision and national security purposes);
 - have a legal system that respect the rule of law, for example ensuring that there are available mechanisms for individuals to obtain (judicial) redress against unlawful government access to personal data;
 - have a comprehensive data protection law or independent data protection authority.

The fourth step is reliant on the result of the third step above. If your assessment under step 3 reveals that the transfer tool is not effective due to the specific circumstances of the third country which the personal data is being transferred you will need to consider additional “supplementary measures” in order to ensure an essentially equivalent level of protection.²³⁷ These supplementary measures will need to be identified on a case-by-case basis. The nature of the supplementary measures may be contractual, technical, organizational or a combination. The EDPB has provided a list of non-exhaustive technical, contractual and organizational measures in Annex 2 of the EDPB [Recommendations 01/2020 on measures that supplement transfer tools](#) to ensure compliance with the EU level of protection of personal data, which you can assess and consider.

Lastly, you must monitor the developments in a third country to which you transferred personal data in order to check whether your initial assessment and decision on the level of protection has been affected or not.

Additional useful resources, tools and further reading:

Further reading:

- EDPB [Recommendations 01/2020 on measures that supplement transfer tools](#) to ensure compliance with the EU level of protection of personal data, Adopted on 10 November 2020.

If an SME responded with a negative answer to this question, then **zero points** would be added to their “GDPR Temperature” and the below recommendation.

Please consider that due to Brexit if your organisation is based in the UK and offers goods or services to EU citizens, then your organisation would be considered as a company that transfers personal data in the EU. Also, keep in mind that remote access from a third country or cloud storage in a cloud situated outside the EEA is also considered a transfer.²³⁸ If this applies to you, change your answer to “Yes” and consider the recommendations.

Q10. Does your company provide employees who carry out data processing activities on your behalf with written instructions (i.e., authorisation to processing of personal data) or training sessions on how to process personal data?

If an SME responded with a positive answer to this question, then the below recommendation would pop up and **zero points** would be added to their “GDPR Temperature”.

In order to guarantee accountability with the GDPR, the data controller shall be able to demonstrate that compliance. In this case you should have evidence that you provided

²³⁶ [Recommendations 01/2020 on measures that supplement transfer tools](#) to ensure compliance with the EU level of protection of personal data, Adopted on 10 November 2020, European Data Protection Board, page 13.

²³⁷ C-311/18 (Schrems II), paragraphs 130 and 133.

²³⁸ [European Data Protection Board Frequently Asked Questions](#) on the judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems, 23 July 2020, FAQ nr. 11.

employees with instructions, for example, by keeping a written record of the persons who have signed an authorisation to process personal data, or by having signed documents of written instructions on data protection for the entire company structure, from high level management to the employees or even candidates (either in their onboarding, or in their specific department / team). Lastly, if you carried out live training sessions or online training courses ensure that you have kept records of the participants of the training or online logs of the attendees.

If an SME responded with a negative answer to this question, then the below recommendation would pop up and **two points** would be **added** to their "GDPR Temperature".

The GDPR does not only focus on technical measures to protect personal data but also organisational safeguards that should raise attention and provide instructions on data protection for the entire company structure, from high level management to the employees or even candidates. Generally, the GDPR specifies that the controller or processor cannot process personal data, except when doing so under instructions from the controller.²³⁹ Therefore, internal company alignment with the expectations and obligations each employee has is integral to lowering a company's risk to compliance. We would recommend to provide short written instructions to employees when they are onboarding the company, including their responsibilities when processing personal data, as well as the necessary precautions they should take when doing their job.

Lastly, an accountable controller should ensure that its employees who are persons authorised are trained in handling personal data and are aware of the main risks that the processing operations may pose to the protection of the personal data. Additionally, these trainings should be demonstrated to the outer world, by for example, organising annual training sessions and keeping records of the participants of the training.

Q11. Does your organisation use suppliers who process personal data on behalf of the organisation?

If an SME responded with a positive answer to this question, then the below recommendation would pop up and **one point** would be **added** to their "GDPR Temperature".

If your company has suppliers who process personal data on behalf of your organisation, then they have to act as data processors. An obligation of the GDPR that falls on the hands of the data controller is to give instructions to data processors and ensure that they comply with the obligations set forth in the GDPR and established by the controller. Therefore, your company, as a data controller should take steps such as signing a Data Protection Agreement, to ensure that the data processor will comply with the necessary safeguards.

If an SME responded with a negative answer to this question, then the below recommendation would pop up and **zero points** would be added to their "GDPR Temperature".

If the answer to question 11. is yes:

11B. Does your organisation provide your suppliers with Data Processing Agreements?

If an SME responded with a positive answer to this question, then **one point** would be **deducted** from their "GDPR Temperature".

As a data controller, you are responsible for the personal data you collect and process – as well as the data that is processed by your chosen data processors. Not having entered into any form of contractual agreements with your processors increases your exposure to sanctions of the GDPR.

We recommend ensuring that the Data Processing Agreement, at least includes:

- the subject-matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data;

²³⁹ Article 29 General Data Protection Regulation.

- the categories of data subjects;
- the obligations and rights of the data controller against the data processor.²⁴⁰

We also suggest keeping an organised archive of the signed DPAs between you as a data controller and your suppliers or service providers as data processors, in order to be able to easily and quickly provide them to the supervisory authority should an investigation arise.

Please mind that violations to controller obligations, such as not properly defining data processors by signing a legally binding contract (or other appropriate legal act) with them, may be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.²⁴¹

Additional useful resources, tools and further reading:

Resources, Tools & Solutions:

- The gdpr.eu project is a project funded by the European Union Horizon 2020 and provides many useful resources for organisations and individuals researching the General Data Protection Regulation. It provides information to help organisations achieve GDPR compliance, including different templates, such as the **template for a Data Processing Agreement**. This template provides a starting point from which your organisation can start in order to create a standard Data Processing Agreement. Your organization can rely on this template, however, you should enhance and complete it, where necessary, with the details of the nature and purpose of the processing, as well as the type of personal data and categories of data subjects.

Further reading:

- [EDPB Guidelines 07/2020](#) on the concepts of controller and processor in the GDPR, Adopted on 02 September 2020.
- [Opinion 1/2010 on the concepts of "controller" and "processor"](#), Adopted on 16 February 2010 by the Article 29 Working Party.

If an SME responded with a negative answer to this question, then the below recommendation would pop up and **two points** would be **added** to their "GDPR Temperature".

As a data controller, you are responsible for the personal data you collect and process – as well as the data that is processed by your chosen data processors. Not having entered into any form of contractual agreements with your processors increases your exposure to sanctions of the GDPR.

We recommend ensuring that you enter into a contract with your processors, under the title of a Data Processing Agreement, which will strictly handle data protection matters and clearly stipulate the instructions of the controller towards the processor. A standard Data Protection Agreement must at least include:

- the subject-matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data;
- the categories of data subjects;
- the obligations and rights of the data controller against the data processor.²⁴²

We also suggest keeping an organised archive of the signed DPAs between you as a data controller and your suppliers or service providers as data processors, in order to be able to easily and quickly provide them to the supervisory authority should an investigation arise.

Please mind that violations to controller obligations, such as not properly defining data processors by signing a legally binding contract (or other appropriate legal act) with them,

²⁴⁰ Article 28 (3) General Data Protection Regulation.

²⁴¹ Article 83 (4) (a) General Data Protection Regulation.

²⁴² Article 28 (3) General Data Protection Regulation.

may be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.²⁴³

Additional useful resources, tools and further reading:

Resources, Tools & Solutions:

- The gdpr.eu project is a project funded by the European Union Horizon 2020 and provides many useful resources for organisations and individuals researching the General Data Protection Regulation. It provides information to help organisations achieve GDPR compliance, including different templates, such as the **template for a Data Processing Agreement**. This template provides a starting point from which your organisation can start in order to create a standard Data Processing Agreement. Your organization can rely on this template, however, you should enhance and complete it, where necessary, with the details of the nature and purpose of the processing, as well as the type of personal data and categories of data subjects.

Further reading:

- [EDPB Guidelines 07/2020](#) on the concepts of controller and processor in the GDPR, Adopted on 02 September 2020.
- [Opinion 1/2010 on the concepts of “controller” and “processor”](#), Adopted on 16 February 2010 by the Article 29 Working Party.

Q12. Have you identified whether the appointment of a Data Protection Officer is mandatory for your organisation?

If an SME responded with a positive answer to this question, **then zero points** would be added to their “GDPR Temperature”.

If an SME responded with a negative answer to this question, then the below recommendation would pop up and **one point** would be **added** to their “GDPR Temperature”.

Your company should at least identify whether having a Data Protection Officer is mandatory or not, seeing as even some SMEs may need to appoint a DPO due to the large-scale processing that they conduct. You will need to designate a data protection officer if:²⁴⁴

- your **core activities** consist of processing personal data, which require **regular and systematic monitoring** of data subjects on a **large scale**; or
- the core activities consist of processing of **special categories of personal data** or **data relating to criminal convictions** and offences, on a **large scale**.

Core activities are the key processing activities to achieve your objectives, for example processing health data can be considered as one of any hospital's core activities.²⁴⁵ On the opposite side are supporting activities, for example IT support, or paying employees, are not considered as core activities for an organization.

In order to establish a processing as “large scale” you needs to consider the factors like²⁴⁶:

- The number of data subjects – either a specific number or as a proportion of the relevant population;
- The volume of data and / or the range of different data items being processed;
- the duration, or permanence, of the data processing activity;
- the geographical scope of the processing activity.

²⁴³ [Article 83 \(4\) \(a\)](#) General Data Protection Regulation.

²⁴⁴ [Article 37 \(1\)](#) General Data Protection Regulation.

²⁴⁵ Guidelines on Data Protection Officers, of the Article 29 Data Protection Working Party, Adopted on 13 December 2016, as last Revised and Adopted on 5 April 2016, page 20.

²⁴⁶ Guidelines on Data Protection Officers, of the Article 29 Data Protection Working Party, Adopted on 13 December 2016, as last Revised and Adopted on 5 April 2016, page 21.

For example, large scale processing ,may include the processing of real time geolocation data of customers, processing customer data in the course of business of an insurance company or a bank, processing personal data for behavioural advertising by a search engine or a social media platform. Processing patient data by a single doctor or physician, or processing personal data relating to criminal convictions and offences by a single lawyer.

Lastly, regular and systematic monitoring includes every form of tracking and profiling online (e.g., behavioural advertising). Some examples of activities that are included in this type of processing are data-driven marketing activities, profiling and scoring for purposes of risk assessment (e.g., for purposes of credit scoring, insurance premiums, fraud prevention), location tracking by mobile apps, monitoring wellness, fitness and health data via wearables, CCTVs, connected devices (e.g., smart meters, smart cars, home automation, etc.).

Overall, the Article 29 Working Party considers 'regular' processing to be one or more of the following²⁴⁷:

- ongoing or occurring at particular intervals for a particular period;
- recurring or repeated at fixed times;
- constantly or periodically taking place.

While the word 'systematic' means one or more of the following²⁴⁸:

- occurring according to a system;
- pre-arranged, organised or methodical;
- taking place as part of a general plan for data collection;
- carried out as part of a strategy.

Additional useful resources, tools and further reading:

Further reading:

- [Guidelines on Data Protection Officers](#), of the Article 29 Data Protection Working Party, Adopted on 13 December 2016, as last Revised and Adopted on 5 April 2016.
- [Guide on Data Protection Officers](#) by the UK Information Commissioner's Officer (ICO).
- [Guidance on appropriate qualifications for a Data Protection Officer](#) (GDPR) by the Irish Data Protection Commission (DPC).
- [Frequently Asked Questions on Data Protection Officers](#) by the Italian Garante.

If the answer to question 12. is yes then:
Q12B. Have you already officially identified and named the Data Protection Officer?

If an SME responded with a positive answer to this question, then **one point** would be **deducted** from their "GDPR Temperature".

It is good practice for the contact details of the DPO to be published in the organisations Privacy Policies and communicated to the competent Supervisory Authority in order for the DPO to be known to them and demonstrate proactivity and cooperation. In addition, you can keep track of the designation of the DPO by the organisation's top management and demonstrate his / her competences through their Curriculum Vitae.

If an SME responded with a negative answer to this question, then the below recommendation would pop up and **one point** would be added to their "GDPR Temperature".

If your company has determined that a DPO is necessary, then it is best that you either hire external advisors as your DPO or appoint an internal function as the DPO of your company. A point to keep in mind should be that whoever takes the role of the DPO should be independent in a way that the DPO does not receive any instructions regarding the exercise of his/her tasks, nor are there any conflicts of interests that may appear in his/her function to

²⁴⁷ Guidelines on Data Protection Officers, of the Article 29 Data Protection Working Party, Adopted on 13 December 2016, as last Revised and Adopted on 5 April 2016, page 21.

²⁴⁸ Guidelines on Data Protection Officers, of the Article 29 Data Protection Working Party, Adopted on 13 December 2016, as last Revised and Adopted on 5 April 2016, pages 21-22.

protect the personal data of the company's data subjects. This entails that the DPO cannot hold another position within the company that it is expected to determine the purposes and means of the processing of personal data, such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of human resources or head of information technology departments.²⁴⁹ Apart from identifying that the Data Protection Officer acts independently, it is also important that when chosen, the DPO acts in accordance with the tasks that are enlisted in the GDPR. In short, the DPO shall:

- inform and advise the controller and employees who carry out processing activities,
- monitor the data protection compliance of the company,
- provide advice to conduct data protection impact assessment,
- act as the contact person for cooperation with the supervisory authority.²⁵⁰

However, the controller remains the one responsible for taking the final decisions with regards to the processing operations.

If you decide to designate a DPO, it is good practice for the contact details of the DPO to be published in the organisations Privacy Policies and communicated to the competent Supervisory Authority in order for the DPO to be known to them and demonstrate proactivity and cooperation. In addition, you can keep track of the designation of the DPO by the organisation's top management and demonstrate his / her competences through their C.V.

Additional useful resources, tools and further reading:

Further reading:

- [Guidelines on Data Protection Officers](#), of the Article 29 Data Protection Working Party, Adopted on 13 December 2016, as last Revised and Adopted on 5 April 2016.
- [Guide on Data Protection Officers](#) by the UK Information Commissioner's Officer (ICO).
- [Guidance on appropriate qualifications for a Data Protection Officer](#) (GDPR) by the Irish Data Protection Commission (DPC).
- [Frequently Asked Questions on Data Protection Officers](#) by the Italian Garante.

Q13. Have you carried out a risk assessment for the processing activities that you conduct; and subsequently have you implemented appropriate technical and organisational measures to ensure and be able to demonstrate that your organisation processes personal data in accordance with GDPR?

If an SME responded with a positive answer to this question, then **two points** would be **deducted** from their "GDPR Temperature".

The risk-based approach that the GDPR has implemented requires all companies evaluate what the risk of each processing activity is, before the processing activity is carried out – that way the company can implement the appropriate technical and organisational measures to ensure a level of security **appropriate to the risk**. The important note for the evaluation of the risk is not only that it indeed occurs but that the company is also able to **demonstrate** that it has occurred. Therefore, we highly recommend keeping track of the risk assessments carried out on the processing activities of the organisation. Additionally, you can make an internal document that describes the security measures that are implemented depending on the risk of the processing activity. Having the document on security measures can also serve helpful for when getting in contact with processors who will need to process personal data on your behalf – since you can immediately provide the security standards you expect from them.

If an SME responded with a negative answer to this question, then the below recommendation would pop up and **two points would be added** to their "GDPR Temperature".

The risk-based approach that the GDPR has implemented requires all companies evaluate what the risk of each processing activity is, before the processing activity is carried out – that way the company can implement the appropriate technical and organisational measures to ensure a level of security **appropriate to the risk**. The important note for the evaluation of

²⁴⁹ Guidelines on Data Protection Officers, of the Article 29 Data Protection Working Party, Adopted on 13 December 2016, as last Revised and Adopted on 5 April 2016, p.16.

²⁵⁰ Art. 39 (1) GDPR.

the risk is not only that it indeed occurs but that the company is also able to **demonstrate** that it has occurred.

Therefore, our practical recommendation is to conduct a risk assessment when you are mapping your processing activities. Furthermore, making a document that describes how the risk assessments are done, for the reason of being able to show the logic in cases of investigations. Additionally, you can make an internal document that describes the security measures that are implemented depending on the risk of the processing activity. Having the document on security measures can also serve helpful for when getting in contact with processors who will need to process personal data on your behalf – since you can immediately provide the security standards you expect from them.

Additional useful resources, tools and further reading:

Resources, Tools & Solutions:

ENISA's customizable online tools for the security of personal data processing:

- [ENISA's risk assessment tool](#) for carrying out risk assessments aims to guide SMEs through their specific data processing activities and help them evaluate the relevant security risks. This tool builds on the existing tools that exist, such as [the CNIL's methodology for privacy risk management](#), ENISA's [recommendations for a methodology of the assessment of severity of personal data breaches](#), and ENISA's [Risk Management and Risk Assessment for SMEs](#) pilot study.
- [ENISA's self assessment of the implemented security measures](#), helps to assess the risk level for a given processing activity and the appropriate security measures taken. This secondary tool can be used as a method of identifying whether the security measures are adequate and to check the status of their implementation.
- An [online tool](#) for cybersecurity in hospitals produced by ENISA. The aim is to help healthcare organisations to quickly identify the most relevant guidelines (such as assets procured or related threats) and promote the importance of a good procurement process to ensure appropriate security measures.

Cyberwatching.eu has identified a list of solutions that are provided from cybersecurity projects, which can increase the level of compliance with the GDPR, of SMEs or other companies. We have analysed a few projects that we believe can be used in order for your organisation to demonstrate technical and organisational measures taken. Please note that some of these projects may not be directly applicable to you and may be specific to a sector in the wider market. Consider that, nowadays, having GDPR measures will add value to your services. The controller has to demonstrate that it works with providers that respect the GDPR – therefore if you are able to guarantee this, then your services will be more valuable.

- [CREDENTIAL](#) is a Secure Cloud Identity Wallet, which provides end-to-end secure and privacy-preserving platform for managing and storing users' digital identity information, ranging from authentication credentials over medical reports to tax data or similar. This solution uses cryptographic mechanisms, as well as determining which of their data goes where. If your SME involves data sharing services, this software may be leveraged as a way to extend your portfolio with privacy enhanced and authenticity.
- [WITDOM's data masking](#) component can be utilised as a security measures for sharing data or for storing data in non-trusted environments. Based on the description given by the WITDOM project, it classifies sensitive data as a direct identifier and instead masks it through a process that creates service-and-user specific tokens that can be updated over time. The Article 29 Working Party has identified three different criteria in order to ensure anonymisation, linkability, singling out and inference. This product satisfies the first requirement, as well as the requirement of irreversibility. As a result, the two requirements of singling out and inference are not fulfilled and therefore this product does not offer anonymisation. Nevertheless, pseudonymisation or masking can be an appropriate security measure to implement – especially if the personal data is in an untrusted environment. Therefore, we would recommend WITDOM's data masking component as a security measure.
- The [DEFEND project](#) provides an innovative data privacy governance platform which supports **healthcare** organizations towards GDPR compliance using

advanced modelling languages and methodologies for privacy-by-design and data protection management. Specific innovations of the project include: the development of advanced modelling languages and methodologies for **privacy-by-design and data protection management**; automated methods and techniques to elicit, map and analyse data that organizations hold for individuals; **integrated encryption and anonymisation solutions for GDPR**; methods and automation techniques for the specification, management and enforcement of personal data consent; a modular solution that covers different aspects of GDPR.

- The [PANACEA project](#) has developed, with three European Healthcare Centres, a people-centric toolkit of nine tools, to **assess and improve the cybersecurity readiness of healthcare socio-technical systems** (ICT, networked medical devices, staff) and of medical device/system lifecycles.
- [SUNFISH platform](#) (Secure Data sharing platform) **provides technical tools to ensure compliance with the EU GDPR**. SUNFISH integrates its data security components with Data Masking services to support only authorised access to the masking/unmasking services, and masked data.
- Axence is an SME that provides professional solutions for the comprehensive management of IT infrastructure for companies and institutions and has a product called [nVision10](#)

Q14. Have you identified the processing activities subject to a Data Protection Impact Assessment ?

If an SME responded with a positive answer to this question, then **one point** would be **deducted** from their “GDPR Temperature”.

Please ensure that the Data Protection Impact Assessments you have carried out are always updated according to the changes and evolution of the processing activity at hand. In addition, you must make sure to be able to demonstrate that you have carried out a DPIA for the high-risk activities, so it would be best practice to always store the specific DPIAs carried out and their evolution.

If an SME responded with a negative answer to this question, then the below recommendation would pop up and **one point** would be **added** to their “GDPR Temperature”.

When a processing operation is likely to result in a high risk to the rights and freedoms of natural persons, a DPIA will be necessary. This is particularly the case when new technologies are being introduced within your company. Other examples of a processing operation that is “likely to result in high risks” are:

- An **automated processing** which uses a **systematic and extensive evaluation of personal aspects** relating to natural persons, including profiling, and on which decisions are based that **produce legal effects** (either to that natural person or significantly affect that person) [more details on what this entails can be found in question 8];
- A processing of **special categories** of personal data, or a processing relating to **criminal convictions** and offences **on a large scale**;
- A **systematic monitoring** of a **publicly accessible area on a large scale**.²⁵¹

When it comes to conducting a DPIA, the French Data Protection Authority has offered a modular tool to conduct the assessment, through a step-by-step process, which can also be customised based on the specific needs of an SME or your business sector. This software is available in both portal and web versions, and can be found for free [here](#).

In order to provide a more concrete set of processing operations that require a DPIA due to their inherent high risk, the GDPR has stipulated that **each Supervisory Authority must draft a public list for the kind of processing operations that should be or should not**

²⁵¹ Guidelines on Data Protection Impact Assessment (DPIA) and determining whoever processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, pg. 8.

be subject to a data protection impact assessment.²⁵² Please check whether your processing activities fall within the activities that must mandatorily carry out a DPIA, which are available [here](#) but also in the designated national supervisory authority's website.

Additional useful resources, tools and further reading:

Resources, Tools & Solutions:

- [A modular tool to conduct Data Protection Impact Assessment](#), through a step-by-step process, which can also be customised based on the specific needs of an SME or your business sector has been created by the French Data Protection Authority. This software is available in both portal and web versions, and can be found for free [here](#).
- [Self assessment checklist for GDPR Readiness Checklist Tool on legal basis](#) (click on "data security") by the Irish Data Protection Commission.

Further reading:

- [Guidelines 05/2020 on Consent](#) under Regulation 2016/679 Version 1.1, Adopted May 2020.
- [Article 29 Working Party Guidelines on consent](#) under Regulation 2016/679, Adopted on November 2017 as last Revised and Adopted on 10 April 2018
- [Guide on Special Category Data](#) by the Information Commissioner's Office (ICO).
- [Guidelines on Data Protection Impact Assessment \(DPIA\)](#) and determining whoever processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.
- [Guide on Data Protection Impact Assessments](#) by the Irish Data Protection Commission.

The methodology of the French Data Protection Authority (CNIL) is a collection of three guides:

- [Privacy Impact Assessment \(PIA\) Methodology](#), which sets out the approach for carrying out a Data Protection Impact Assessment.
- [Privacy Impact Assessment \(PIA\) Templates](#), including information that can be used to carry out the analysis of the Data Protection Impact Assessment.
- [Privacy Impact Assessment \(PIA\) Knowledge Bases](#), a catalogue of controls aimed at complying with the legal requirements and mitigating the risks.

If the answer to question 14 is yes, then:

14B. Have you already conducted the Data Protection Impact Assessment?

If an SME responded with a positive answer to this question, then **one point** would be **deducted** from their "GDPR Temperature".

Please ensure that the Data Protection Impact Assessments you have carried out are always updated according to the changes and evolution of the processing activity at hand. In addition, you must make sure to be able to demonstrate that you have carried out a DPIA for the high-risk activities, so it would be best practice to always store the specific DPIAs carried out and their evolution.

If an SME responded with a negative answer to this question, then the below recommendation would pop up and **half a point** would be **added** to their "GDPR Temperature".

When it comes to conducting a DPIA, the French Data Protection Authority has offered a modular tool to conduct the assessment, through a step-by-step process, which can also be customised based on the specific needs of an SME or your business sector. This software is available in both portal and web versions and can be found for free [here](#).

Additional useful resources, tools and further reading:

Resources, Tools & Solutions:

- [A modular tool to conduct Data Protection Impact Assessment](#), through a step-by-step process, which can also be customised based on the specific needs of an SME or your business sector has been created by the French Data Protection Authority.

²⁵² Articles 35 (5) and (6) General Data Protection Regulation.

This software is available in both portal and web versions, and can be found for free here.

- [Self assessment checklist for GDPR Readiness Checklist Tool on legal basis](#) (click on “data security”) by the Irish Data Protection Commission.

Further reading:

- [Guidelines 05/2020 on Consent](#) under Regulation 2016/679 Version 1.1, Adopted May 2020.
- [Article 29 Working Party Guidelines on consent](#) under Regulation 2016/679, Adopted on November 2017 as last Revised and Adopted on 10 April 2018
- [Guide on Special Category Data](#) by the Information Commissioner's Office (ICO).
- [Guidelines on Data Protection Impact Assessment \(DPIA\)](#) and determining whoever processing is “likely to result in a high risk” for the purposes of Regulation 2016/679.
- [Guide on Data Protection Impact Assessments](#) by the Irish Data Protection Commission.

The methodology of the French Data Protection Authority (CNIL) is a collection of three guides:

- [Privacy Impact Assessment \(PIA\) Methodology](#), which sets out the approach for carrying out a Data Protection Impact Assessment.
- [Privacy Impact Assessment \(PIA\) Templates](#), including information that can be used to carry out the analysis of the Data Protection Impact Assessment.
- [Privacy Impact Assessment \(PIA\) Knowledge Bases](#), a catalogue of controls aimed at complying with the legal requirements and mitigating the risks.

Q15. Have you assessed whether your organisation is obliged to keep records of processing activities ?

If an SME responded with a positive answer to this question, then **one point** would be **deducted** from their “GDPR Temperature”.

The GDPR stipulates the obligation that each controller and processor must maintain a record of processing activities. It is recommended that you keep this record updated regularly, according to the functional and practical evolving of data processing. In practice, if new data is collected, if the retention period is changed, or if a new processing recipient is involved, this must be added to the record.²⁵³

Additional useful resources, tools and further reading:

Resources, Tools & Solutions:

- [A template of the record of processing activities](#) has been developed by the Cypriot Office of the Commissioner for Personal Data Protection.
- [A template of record of processing activities](#) which has been developed by the French Commissioner National Protection Authority (CNIL) that provides a template for both data controllers and data processors.

If an SME responded with a negative answer to this question, then the below recommendation would pop up and **half a point** would be **added** to their “GDPR Temperature”.

The GDPR stipulates the obligation that each controller and processor must maintain a record of processing activities. Nevertheless, it has created an exemption for any enterprise or organisation that employs fewer than 250 persons.²⁵⁴ However, if your company conducts one of the three following types of processing, then this exception does **not** apply to you:

- If the processing is likely to result in **a risk** to the rights and freedoms of data subjects (you can assess this by conducting a short risk assessment, to check if any risk at all occurs);

²⁵³ Commission Nationale de l'Informatique et des Libertés, [Record of Processing Activities](#).

²⁵⁴ Working Party 29 Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Art. 30 (5) GDPR.

- If the processing is **not occasional**;
- If the processing **includes special categories** of data or personal **data relating to criminal convictions and offences**.

Therefore, as an SME, it is vital that you check whether one of the three above cases apply to you, since you will then be obliged to keep a record of processing activities. If you do not ensure that you indeed fall into the category of being exempt from the obligation of keeping record of all processing activities, then you will be subject to GDPR sanctions.

If the answer to question 15 is yes then:
Q15B. If you have assessed it and you are obliged to keep the records of processing activities, have you already filled out the records?

If an SME responded with a positive answer to this question, then **two points** would be **deducted** from their "GDPR Temperature".

If an SME responded with a negative answer to this question, then the below recommendation would pop up and **one point** would be **added** to their "GDPR Temperature".

The record of processing activities should contain at least the following information, if you are a data controller:²⁵⁵

- The name and contact details of the controller;
- The name and contact details of the data protection officer, if applicable;
- The purposes of the processing;
- A description of the categories of data subjects;
- A description of the categories of personal data;
- The categories of recipients to whom the personal data have been or will be disclosed;
- Transfers of personal data to a non-EU country, where applicable.

Furthermore, the records of processing activities should contain at least the following information, if you are a data processor:²⁵⁶

- The name and contact details of the processor or processors, and of each controller on behalf of which the processor is acting;
- The name and contact details of the data protection officer, if applicable;
- A description of the categories of processing carried out on behalf of each controller;
- Transfers of personal data to a non-EU country, where applicable;
- A general description of the technical and organisational security measures.

If you are obliged to keep a record of processing, it is recommended that you keep the record updated regularly, according to the functional and practical evolving of data processing. For example, if new data is collected, if the retention period is changed, or if a new processing recipient is involved, this must be added to the record.²⁵⁷

Additional useful resources, tools and further reading:

Resources, Tools & Solutions:

- [A template of the record of processing activities](#) has been developed by the Cypriot Office of the Commissioner for Personal Data Protection.
- [A template of record of processing activities](#) which has been developed by the French Commissioner National Protection Authority (CNIL) that provides a template for both data controllers and data processors.

Q16. Has your organisation developed a personal data breach management procedure that includes the related notifications and communications?

If an SME responded with a positive answer to this question, then **two points** would be **deducted** from their "GDPR Temperature".

Since you have already developed a personal data breach management procedure it is recommended that you make sure to keep track of any incidents that have occurred (even

²⁵⁵ Art. 30 (1) GDPR.

²⁵⁶ Art. 30 (2) GDPR.

²⁵⁷ Commission Nationale de l'Informatique et des Libertés, [Record of Processing Activities](#).

those that you have labelled as not personal data breaches) and the mitigating actions taken or notifications sent to the supervisory authority or data subjects, through for a register of personal data breaches. It is also suggested that you harmonise and possibly integrate the data breach procedure with any eventual cybersecurity incident handling procedure.

Additional useful resources, tools and further reading:

Resources, Tools & Solutions:

- [Self assessment checklist for GDPR Readiness Checklist Tool on legal basis](#) (click on “data security”) by the Irish Data Protection Commission.
- [GuardYoo](#) is an automated compromise assessment platform developed by an SME. Based on the information provided, it is a solution for forensics analysis of the network, and it seems to deliver an audit relatively shortly, within 1 week, in comparison to how long it would take for a consulting team to carry it out (4-8 weeks), it is still not considered GDPR compliant. In order to ensure that a personal data breach is detected as soon as possible it would need to immediately alert of such event. However, this may be unrealistic and therefore, this tool can act as a preventative – bird-eye vision of the network. However, there would need to be another system in place in order to ensure that the personal data breach is detected as soon as possible and communicated to the supervisory authority or the data subjects (should there be a high risk to the data subject) within 72 hours.

If an SME responded with a negative answer to this question, then the below recommendation would pop up and **two points** would be **added** to their “GDPR Temperature”.

It is needless to say that when a data breach occurs, it is not a moment where a company can improvise its reaction, therefore, it is of extreme importance to have it figured out before it actually happens. The GDPR gives the timeline of notifying the supervisory authority of the data breach within 72 hours, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the data subjects. For these reasons you need to have protocol, or a procedure determined in order to recognise **when** a data breach has occurred, **how** it will be recognised, **how** the company will react to it, and **who** will be involved in these steps. The answers to the above questions will result to a procedure on data breach management. In defining a procedure on data breach management, we suggest taking into consideration the evaluation of the likelihood that the breach results in risks to the rights and freedoms of the data subjects by applying:

- the accountability principle set forth in the GDPR in order to be able to demonstrate the responsiveness and actions taken as a result of a personal data breach to the supervisory authority, by at least documenting any personal data breaches and subsequent actions including: a) the facts relating to the personal data breach, b) its effects to data subjects and, c) the remedial action taken.²⁵⁸
- the methodology provided by the European Agency for Network and Information Security (ENISA) to assess the severity of personal data breaches by taking into account:
 - 1) the data processing context, i.e., the type of data breached, and the overall processing operation,
 - 2) the ease of identification of the data subjects from the data involved in the breach,
 - 3) the specific circumstances of the breach, for example, whether it is a loss of confidentiality, or any malicious intent that may be involved.²⁵⁹

In addition to notifying the supervisory authority, according to Article 34(1) of the GDPR, the data controller is also required to communicate a breach to the affected individuals, “when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons”. The communication should be done as soon as possible (namely “without undue delay”) and aims to provide individuals with specific information about the steps they should take to protect themselves. This could also be done by providing specific advice to individuals to protect themselves from adverse consequences of the breach (for instance, resetting passwords).

²⁵⁸ Guidelines on Personal data breach notification under Regulation 2016/679, p.23.

²⁵⁹ Recommendations for a methodology of the assessment of severity of personal data breaches, p. 9.

Furthermore, breaches should be communicated to the concerned individuals directly with dedicated and transparent methods of communication which can ensure individuals understand the information being provided to them (e.g., email, SMS or prominent website banners in relevant languages).

Notification to individuals is not required when:

- the controller has applied appropriate technical and organisational measures to protect personal data prior to the breach (such as state-of-art encryption);
- immediately following a breach, the controller has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise;
- it would involve disproportionate effort to contact individuals.

It is recommended that you make sure to keep track of any incidents that have occurred (even those that you have labelled as not personal data breaches) and the mitigating actions taken or notifications sent to the supervisory authority or data subjects, through for a register of personal data breaches. It is also suggested that you harmonise and possibly integrate the data breach procedure with any eventual cybersecurity incident handling procedure.

If controllers fail to notify the data breach to the supervisory authority or to communicate it to the data subjects (infringement of Articles 33 and 34 of the GDPR), the supervisory authority will have the possibility to issue administrative fines, whose value can be up to 10,000,000 EUR or up to 2 % of total worldwide annual turnover (Article 83 (4)(a)). Nevertheless, where the failure to notify a breach reveals an absence or inadequacy of existing security measures, the supervisory authority may also issue sanctions for the infringement of Article 32 of the GDPR.

Additional useful resources, tools and further reading:

Resources, Tools & Solutions:

- [Self assessment checklist for GDPR Readiness Checklist Tool on legal basis](#) (click on "data security") by the Irish Data Protection Commission.
- [The Data breach notification tool](#) developed by the Italian Garante.
- Fitsec Ltd is a Finnish cyber security company that offers cybersecurity services, including the [Asset tracker](#) which can be found in Cyberwatching.eu's Marketplace. The Asset tracker assists organisations in detecting their data leaks. Specifically, this service enables them to track personal data of an organisation and check if the data has leaked to the internet. Tracking this information for an organisation that handle personal data enables the organisation not only to have a quick response to the Supervisory Authority (within 72 hours of the personal data breach) but it also helps minimize the risks to the data subjects. In addition, the SME can help isolate and fix weaknesses in the organisation's security in order to ensure that the security gap has been adequately filled. The service also helps organizations to fulfil the requirement of notifying affected parties in the event of a data breach, as outlined in the GDPR. Assets, or information related to the organization can be for example: email addresses, IP addresses, domain names or payment card information. The service is easy to use and does not require any installations in your environment. From the easy-to-use [web interface](#), you can see the assets being monitored, add new assets to be monitored and analyse any matches that have been found. All findings are reported to you in whatever way you desire.
- [GuardYoo](#) is an automated compromise assessment platform developed by an SME. Based on the information provided, it is a solution for forensics analysis of the network, and it seems to deliver an audit relatively shortly, within 1 week, in comparison to how long it would take for a consulting team to carry it out (4-8 weeks), it is still not considered GDPR compliant. In order to ensure that a personal data breach is detected as soon as possible it would need to immediately alert of such event. However, this may be unrealistic a therefore, this tool can act as a preventative – bird-eye vision of the network. However, there would need to be another system in place in order to ensure that the personal data breach is detected

as soon as possible and communicated to the supervisory authority or the data subjects (should there be a high risk to the data subject) within 72 hours.

Further reading

- [Recommendations for a methodology of the assessment of severity of personal data breaches](#), developed by ENISA, Greek and German Data Protection Authority.
- [Guide on personal data breach management and notification](#), developed by Spanish Data Protection Authority (AEPD).
- [72 hours how to respond to a personal data breach](#) – a simple guide for small companies by the UK Information Commissioner's Office (ICO).

ANNEX B. SURVEY AND RECOMMENDATIONS FOR INFORMATION NOTICES

Please complete the questions below in order to assess whether your information notice is complete

1. Does the information notice specify **who** decides how the data subject's personal data can be used and for which **purposes**?
 - ☐ Yes, this information is provided
 - ☐ No, this information is missing
 - ☐ Not applicable

Where the respondent picked the positive answer, the below recommendation would come up.

If your organisation decides how the data subject's personal data can be used, meaning the **means** with which it will be processed (i.e., software, hardware, specific instructions on the use of these data) and for which **purposes** it may be used (i.e., why is the processing of this personal data taking place), then most likely you are a data controller under the GDPR.²⁶⁰ If you are a controller, as per the above definition, the obligation to provide information to the data subject concerning the processing of their personal data falls on you. Regardless of whether you have collected the personal data directly from the data subject, or, indirectly from another person, this obligation remains with the only difference being that in the latter case the controller shall provide the information either 1) within a **reasonable period** after obtaining the personal data, but at the latest within one month, or, 2) at the time of the **first communication** to that data subject.

From the other hand, if you do not fall within the definition of a data controller, but instead you receive instructions in order to process personal data on behalf of a controller (who determines the means and purposes of the processing), then your role is that of the data processor. In this case, you will need to count on the data controller to provide to the data subject the relevant information. Please be cautious of the cases where you may take the role of the data controller, meaning where you fail to fulfil the instructions given by the controller, or where you determine your own purpose and means of the processing – then you are considered a data controller under the GDPR.²⁶¹ This means that for the cases where you are a data controller the obligation to provide information to the data subject will apply to you.

Where the respondent picked the N/A answer, the below recommendation would come up.

If you receive instructions in order to process personal data on behalf of a controller (who determines the means and purposes of the processing), then your role is that of the data processor. In this case, you will need to count on the data controller to provide to the data subject the relevant information. Please be cautious of the cases where you may take the role of the data controller, meaning where you fail to fulfil the instructions given by the controller, or where you determine your own purpose and means of the processing – then you are considered a data controller under the GDPR.²⁶² This means that for the cases where you are a data controller the obligation to provide information to the data subject will apply to you.

Where the respondent picked the negative answer, the below recommendation would come up.

Providing an information notice or a privacy policy is essential according to the GDPR (Articles 13 and 14). As an entity that processes personal data of data subjects, you have the obligation to inform your data subjects, **at the time when the personal data are obtained**, of specific aspects of the processing activity. One of the core information that must be communicated to the data subject is the purposes for which you process their data, and who decides these purposes (depending on whether you are a controller or a processor).

²⁶⁰ Art. 4 (7) General Data Protection Regulation.

²⁶¹ Art. 28 (10) General Data Protection Regulation.

²⁶² Article 28 (10) General Data Protection Regulation.

2. Does the information notice indicate the identity and the contact details of the controller?
- ☐ Yes, this information is provided
- ☐ No, this information is missed

Where the respondent picked the negative answer, the below recommendation would come up.

It is recommended to integrate the information notice with this information, essential according to Article 13 (1) (a) and Article 14 (1) (a) GDPR. In fact, it is necessary for the controller's identity and contact details to be disclosed to the data subject; in that way the data subject may contact the controller if any questions, or complains arise in the handling of their personal data.

3. Does the information notice provide the contact details of the DPO, if one has been appointed?
- ☐ Yes, this information is provided
- ☐ No, this information is missed
- ☐ Not applicable (No DPO appointed)

Where the respondent picked the negative answer, the below recommendation would come up.

The contact details of the Data Protection Officer must be provided in the information notice, according to Article 13 (1) (b), and Article 14 (1) (b) GDPR.

Where the respondent picked the answer that it is not applicable, the below recommendation would come up.

If you have not assessed whether you need to appoint a DPO, and you are an SME, click [here](#)²⁶³ to fill out a further survey that will give you further advice on how to handle this matter, if you are a Research and Innovation Project click [here](#).²⁶⁴

4. Does the information notice explain **how** the personal data are processed, meaning for which **purposes**?
- ☐ Yes, this information is provided
- ☐ No, this information is missed

Where the respondent picked the positive answer, the below recommendation would come up.

Well done! Remember to also specify the legal basis you have decided to rely on for **each purpose** you mention (see next question for more details on that).

Where the respondent picked the negative answer, the below recommendation would come up.

It is recommended to integrate the information notice with this information, essential according to Article 13 (1) (c) and Article 14 (1) (c) GDPR.
The purposes of the processing for which the personal data are intended is necessary to be disclosed, in order for the data subject to have the ability to understand why they shall provide you with their personal data.²⁶⁵

²⁶³ The link will lead to the survey described in section 3.1 of this deliverable.

²⁶⁴ The link will lead to the survey described in section 3.3 of this deliverable.

²⁶⁵ Article 13 (1) (c) and Art. 14 (1) (c) General Data Protection Regulation.

5. Does the information notice include the **legal basis** of the processing?

- ☐ Yes, this information is provided
☐ No, this information is missed

Where the respondent picked the negative answer, the below recommendation would come up.

It is recommended to integrate the information notice with this information, essential according to Article 13 (1) (c) and Article 14 (1) (c) GDPR.

The legal basis of the processing of personal data must be disclosed to the data subject, in this way utmost transparency is offered.²⁶⁶ In order to ensure a smooth relationship with your data subject, and to enhance transparency, it will be vital for the data subject not only to understand what and how you process the personal data but also to know that it is done in a **legal** manner. There is a variety of legal basis that can be used in order to process personal data, such as consent, the performance of a contract, compliance with a legal obligation, or due to the legitimate interest of your organisation.

You can also use the [lawful basis interactive tool](#) produced by the Information Commissioner's Office (ICO). It is a **useful interactive tool to receive tailored guidance on which lawful basis is likely to be the most appropriate for your processing activities**. This tool will result to a rating for each lawful basis based on the answers to key questions, accompanied by suggestions on the actions you should take.

6. If any processing is based on the **legitimate interest** of your organisation, does the information notice explain what this legitimate interest involve?

- ☐ Yes, this information is provided
☐ No, this information is missed
☐ Not applicable (no processing is based on the legitimate interest of the organisation)

Where the respondent picked the negative answer, the below recommendation would come up.

It is recommended to integrate the information notice with this information, essential according to Article 13 (1) (d) and Article 14 (2) (b) GDPR.

It is important to note that where you choose to utilise the legal basis of **legitimate interest**, then the **specific legitimate interest pursued** must be explained to the data subject – this includes a description of the reason for this legitimate interest.²⁶⁷

According to the Article 29 Working Party an interest is the interest or benefit that the controller gets (or the society too) as a result of the processing.²⁶⁸ The decision to rely on legitimate interest as a legal basis must be the result of a proper evaluation of a) whether the company has a legitimate interest, b) whether the processing is necessary for that specific legitimate interest and c) whether the legitimate interest overrides the interests and rights of the data subject. As you may have noticed, you need to carry out a balancing test between the legitimate interest of your organization and the interests and fundamental rights of the data subjects involved. In addition, the interest must be “real” and “present”, meaning that it must correspond with the current activities of your organization, or, at least, the expected benefits should be realized in the very near future. Therefore, the interest must be specific and should not be assumed. It is important to explain the legitimate interest to the data subject because the nature of a company's interest can vary (for example, the legitimate interest to carry out scientific research is completely different from the economic interest of

²⁶⁶ Article 13 (1) (c) and Art. 14 (1) (c) General Data Protection Regulation.

²⁶⁷ Article 13 (1) (d) and Art. 14 (2) (b) General Data Protection Regulation.

²⁶⁸ Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p.23, available here: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm.

an organization to learn as much as possible about its potential customers so that it can create more successful targeted advertisement about its products and or services.²⁶⁹

After having carried out the necessary assessments which resulted to the use of legitimate interest as a legal basis for the processing it is crucial to inform your data subjects about it in a **clear** and **user-friendly manner**. This way the data subjects will be enabled to exercise their rights.

You can also use the [lawful basis interactive tool](#)²⁷⁰ produced by the Information Commissioner's Office (ICO). It is a **useful interactive tool to receive tailored guidance on which lawful basis is likely to be the most appropriate for your processing activities**. This tool will result to a rating for each lawful basis based on the answers to key questions, accompanied by suggestions on the actions you should take.

7. Does the information notice indicate which personal data are processed? (i.e., name, contact details, official governmental documents, health data, etc.)
- ☐ Yes, this information is provided
 - ☐ No, this information is missed

Where the respondent picked the negative answer, the below recommendation would come up.

The disclosure of the personal data processed is not required in the scenario where you collected the personal data directly from the data subject.

However, in case where you have **not** obtained the personal data from the data subject directly (i.e., you have received it from a third person or from another organisation), then it is recommended to integrate the information notice with this information, essential according to Article 14(1)(e) GDPR. If it is not possible to disclose the exact personal data processed due to the large amount, or because it is determined in an ad hoc basis, then you may simply state the **categories of personal data** concerned.²⁷¹ Some categories of personal data include, contact details, political opinions, health data, religious data and so on.

8. Does the information notice indicate with whom the personal data are shared, if any?
- ☐ Yes, this information is provided
 - ☐ No, this information is missed
 - ☐ Not applicable (the personal data are not shared)

Where the respondent picked the negative answer, the below recommendation would come up.

It is recommended to integrate the information notice with this information, essential according to Article 13 (1) (e) and Article 14 (1) (e) GDPR.

The best case would be for the recipients of the personal data to be explicitly listed to the data subject. However, if this is not possible, then the GDPR allows for simply the categories of the recipients to be disclosed, as long as the clustering of the recipients is truthful and without excluding specific categories for internal purposes.

9. Does the information indicate if your organisation intends to transfer the personal data outside the European Economic Area? If you do transfer personal data, does it additionally include the appropriate transfer tools and safeguards on which the is transfer based?
- ☐ Yes, this information is provided

²⁶⁹ Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p.23, available here:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm.

²⁷⁰ <https://ico.org.uk/for-organisations/gdpr-resources/lawful-basis-interactive-guidance-tool/>.

²⁷¹ Article 14 (1) (d) General Data Protection Regulation.

- ☐ No, this information is not provided
☐ Not applicable (no transfers take place)

Where the respondent picked the **positive** answer, the below recommendation would come up.

Please keep in mind that it is necessary to **specify** the safeguard the transfer is based on, for example, whether you rely on an adequacy decision, Standard Contractual Clauses, Codes of Conduct, etc.

Furthermore, please consider that due to Brexit if your organisation is based in the UK and offers goods or services to EU citizens, then your organisation would be considered as a company that transfers personal data in the EU. On June 28th 2021 the United Kingdom received an adequacy decision from the European Commission which means that if your organisation transfers personal data outside the European Economic Area (EEA) to the United Kingdom you must specify that the transfer tool you rely on is the adequacy decision.²⁷² Also, keep in mind that remote access from a third country or cloud storage in a cloud situated outside the EEA is also considered a transfer.²⁷³

Lastly, also note that due to the Schrems II ruling issued on July 2020 there are additional steps that must be taken when transfers take place.

1. Identify your transfers;
2. Identify the transfer tool you rely on;
3. Is the tool effective in the place of destination;
4. If the tool is not effective, supplementary safeguards must identified;
5. The above safeguards must be put in place (organisational, contractual, technical measures);
6. A regular re-evaluation of the level of protection should be carried out.

If you would like to check your compliance with the GDPR or receive more detailed recommendations on the topic of transfers, you can take the assessment of the [GDPR Temperature Tool](#) and specifically Question 9.

Where the respondent picked the negative answer, the below recommendation would come up.

It is recommended to integrate the information notice with this information, essential according to Article 13 (1) (f) and Article 14 (1) (f) GDPR.

If you **intend** to transfer personal data outside the European Union, this needs to be clearly disclosed to the data subject. It is especially important to further explain the existence of the safeguards implemented in order for the transfers to legally take place – safeguards may include: an adequacy decision by the Commission, or binding corporate rules, standard contractual data protection clauses adopted by the Commission, an approved code of conduct, or an approved certification mechanism.²⁷⁴

Furthermore, please consider that due to Brexit if your organisation is based in the UK and offers goods or services to EU citizens, then your organisation would be considered as a company that transfers personal data in the EU. On June 28th 2021 the United Kingdom received an adequacy decision from the European Commission which means that if your

²⁷² Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, available at: https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf.

²⁷³ [European Data Protection Board Frequently Asked Questions](#) on the judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems, 23 July 2020, FAQ nr. 11.

²⁷⁴ Article 13 (1) (f), Art. 14 (1) (f) and Art. 46 (2) (b), (c), (d), (e), (f) General Data Protection Regulation.

organisation transfers personal data outside the European Economic Area (EEA) to the United Kingdom you must specify that the transfer tool you rely on is the adequacy decision.²⁷⁵ Also, keep in mind that remote access from a third country or cloud storage in a cloud situated outside the EEA is also considered a transfer.²⁷⁶

Lastly, also note that due to the Schrems II ruling issued on July 2020 there are additional steps that must be taken when transfers take place.

1. Identify your transfers;
2. Identify the transfer tool you rely on;
3. Is the tool effective in the place of destination;
4. If the tool is not effective, supplementary safeguards must identified;
5. The above safeguards must be put in place (organisational, contractual, technical measures);
6. A regular re-evaluation of the level of protection should be carried out.

If you would like to check your compliance with the GDPR or receive more detailed recommendations on the topic of transfers, you can take the assessment of the [GDPR Temperature Tool](#) and specifically Question 9.

Where the respondent picked the N/A answer, the below recommendation would come up.

Please consider that due to Brexit if your organisation is based in the UK and offers goods or services to EU citizens, then your organisation would be considered as a company that transfers personal data in the EU. Also, keep in mind that remote access from a third country or cloud storage in a cloud situated outside the EEA is also considered a transfer.²⁷⁷ If this applies to you, change your answer to “No” and consider the recommendations.

10. Does the information notice indicate for how long the personal data are stored?

- ☐ Yes, this information is provided
- ☐ No, this information is missed
- ☐ ~~Not applicable~~

Where the respondent picked the negative answer, the below recommendation would come up.

It is recommended to integrate the information notice with this information, essential according to Article 13 (2) (a) and Article 14 (2) (a) GDPR.

In order to ensure a fair and transparent processing in respect of the data subject, **the period** for which the personal data will be stored **for each purpose** earlier identified should be explained to the data subject. This specification is due to the fact that it is logical that different purposes of processing may also have a different retention period. Sometimes, **the criteria used** to determine the retention period may be sufficient, if it is not possible to describe the retention period to the data subject.²⁷⁸

In addition, order to guarantee that the personal data is deleted following the expiration of the retention period defined it is recommended to adopt a data retention policy. This data

²⁷⁵ Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, available at: https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf.

²⁷⁶ [European Data Protection Board Frequently Asked Questions](#) on the judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems, 23 July 2020, FAQ nr. 11.

²⁷⁷ [European Data Protection Board Frequently Asked Questions](#) on the judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems, 23 July 2020, FAQ nr. 11.

²⁷⁸ Article 13 (2) (a), Article 14 (2) (a) General Data Protection Regulation.

retention policy will not only better define and specify the retention periods but it can also explain which organizational and technical measures your organization has put in place to respect the retention periods defined.

Where the respondent picked the positive answer, the below recommendation would come up.

Well done! In order to guarantee that the personal data is deleted following the expiration of the retention period defined it is recommended to adopt a data retention policy. This data retention policy will not only better define and specify the retention periods, but it can also explain which organizational and technical measures your organization has put in place to respect the retention periods defined.

11. Does the information notice explain the existence of automated decision-making used to make decisions based solely on automated processing (including profiling), which produces legal effects concerning the data subject or similarly significantly affects him / her?

- ☐ Yes, this information is provided
- ☐ No, this information is missed
- ☐ Not applicable (the processing does not involve any automated decision-making, including profiling)

Where the respondent picked the positive answer, the below recommendation would come up.

Good job! Remember to explain **clearly** and **simply** to individuals how the profiling or automated decision-making works.²⁷⁹ In short: you must check whether your explanation offers meaningful information about the logic involved. If your processing involves profiling-based decision making, then it must be clarified to the data subject that the processing takes place for **both purposes** (a) profiling, and (b) making a decision based on the profile generated.²⁸⁰ Additionally, the data subject should be informed not only about a right *to be informed* about but also, in certain circumstances, a right *to object to profiling*, regardless of whether it is solely automated individual decision-making based on profiling takes place.²⁸¹ You must provide information about intended or future processing, and how the automated decision-making might affect the data subject – the significant and the envisaged data protection consequences.²⁸² In order for this information to be understandable by any data subject, it must be accompanied with examples of the type of possible effects. Taking the example given by the Working Party 29 in the Guidelines on Automated individual decision-making and Profiling: an insurance company uses an automated decision-making process to set motor insurance premiums based on monitoring customers' driving behaviour. It provides an app comparing fictional drivers (including ones with dangerous habits) in order to illustrate the significant and envisaged consequences of the automated-decision processing they would like to use.²⁸³ The Guidelines on Automated individual decision-making and Profiling further advice that other visual techniques may be used to explain how a paste decision has been made, that way the data subject can clearly conceive the consequences.

As a controller, you may carry out profiling and automated decision-making so long as you respect all the principles and have a proper legal basis for the processing. Please make sure that you have also carried out a Data Protection Impact Assessment, since automated decision-making activities may often lead to high risks for the data subjects. Carrying out a

²⁷⁹ Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, as last Revised and Adopted on 6 February 2018, p.16.

²⁸⁰ Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, as last Revised and Adopted on 6 February 2018, p.16.

²⁸¹ Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, as last Revised and Adopted on 6 February 2018, p.17.

²⁸² Art. 13 (2) (f), Art. 14 (2) (g) General Data Protection Regulation.

²⁸³ Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, as last Revised and Adopted on 6 February 2018, p.26.

DPIA will both enable you to assess the risks of the processing activity, as well as demonstrate that you have put in place appropriate measures to address those risks.²⁸⁴ If you would like to check your compliance with the GDPR or receive more detailed recommendations on the topic of automated decision-making, you can take the assessment of the [GDPR Temperature Tool](#) and specifically Question 8.

Where the respondent picked the negative answer, the below recommendation would come up.

It is recommended to integrate the information notice with this information, essential according to Article 13 (2) (f) and Article 14 (2) (g) GDPR.

The GDPR stipulates that the data subject shall have the right **not to be subject** to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.²⁸⁵ Therefore, if you plan to conduct any automated individual decision-making (that produces legal effects to the data subject), the only way to do so is if the decision:

- is necessary for entering into, or performance of, a contract between the data subject and a data controller; or
- is authorised by European or Member State law to which the controller is subject to and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- is based on the data subject's explicit consent.²⁸⁶

Profiling is composed of three elements: 1) it has to be an **automated** form of processing; 2) it has to be carried out on **personal data**; 3) the objective of the profiling must be to **evaluate personal aspects** about a natural person.²⁸⁷ An example of profiling may be a data broker collecting data from different public and private sources, on behalf of its clients or for its own purposes, with the purpose of compiling the data to develop profiles on the individuals in order to eventually place them into segments.

Solely automated decision-making has a different scope, in that it is the ability to make decisions by technological means, without human involvement. For example, giving out speeding fines purely on the basis of evidence gathered from speed cameras.

If you employ solely automated decision-making, including profiling, which produces legal effects concerning the data subject, or similarly significantly affecting him / her, then you must ensure to explain **clearly** and **simply** to individuals how the profiling or automated decision-making works.²⁸⁸ In short: you must offer meaningful information about the logic involved.

If the processing involves profiling-based decision making, then it must be clarified to the data subject that the processing takes place for **both purposes** (a) profiling, and (b) making a decision based on the profile generated.²⁸⁹

Additionally, the data subject should be informed not only about a right *to be informed* about but also, in certain circumstances, a right *to object to profiling*, regardless of whether it is solely automated individual decision-making based on profiling takes place.²⁹⁰

As a controller, you may carry out profiling and automated decision-making so long as you respect all the principles and have a proper legal basis for the processing. Please make sure

²⁸⁴ Guidelines on Automated individual decision-making and profiling, for the purposes of Regulation 2016/679, pg. 29.

²⁸⁵ Art. 22 (1) GDPR.

²⁸⁶ Art. 22 (2) GDPR.

²⁸⁷ Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, as last Revised and Adopted on 6 February 2018, p.6-7.

²⁸⁸ Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, as last Revised and Adopted on 6 February 2018, p.16.

²⁸⁹ Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, as last Revised and Adopted on 6 February 2018, p.16.

²⁹⁰ Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, as last Revised and Adopted on 6 February 2018, p.17.

that you have also carried out a Data Protection Impact Assessment, since automated decision-making activities may often lead to high risks for the data subjects. Carrying out a DPIA will both enable you to assess the risks of the processing activity, as well as demonstrate that you have put in place appropriate measures to address those risks.²⁹¹

If you would like to check your compliance with the GDPR or receive more detailed recommendations on the topic of automated decision-making, you can take the assessment of the [GDPR Temperature Tool](#) and specifically Question 8.

If answer to Q11. is Yes:

Q11B. Does the information notice contain an explanation of the consequences for the data subject, as a result of the automated decision-making?

- ☐ Yes, this information is provided
- ☐ No, this information is missed
- ☐ Not applicable

Where the respondent picked the negative answer, the below recommendation would come up.

You must provide information about intended or future processing, and how the automated decision-making might affect the data subject – the significant and the envisaged data protection consequences.²⁹² In order for this information to be understandable by any data subject, it must be accompanied with examples of the type of possible effects. Taking the example given by the Working Party 29 in the Guidelines on Automated individual decision-making and Profiling: an insurance company uses an automated decision-making process to set motor insurance premiums based on monitoring customers' driving behaviour. It provides an app comparing fictional drivers (including ones with dangerous habits) in order to illustrate the significant and envisaged consequences of the automated-decision processing they would like to use.²⁹³ The Guidelines on Automated individual decision-making and Profiling further advice that other visual techniques may be used to explain how a paste decision has been made, that way the data subject can clearly conceive the consequences.

12. Does the information notice explain whether the data are further processed for a purpose other than that for which they were obtained?

- ☐ Yes, this information is provided
- ☐ No, this information is missed
- ☐ Not applicable (the data are not further processed for a purpose other than that for which they were obtained)

Where the respondent picked the negative answer, the below recommendation would come up.

If your organisation intends to further process the personal data for a purpose other than that for which the personal data were collected, it is recommended to provide the data subject with information on that other purpose and with any relevant further information **prior to that further processing**, according to Article 13 (3) and Article 14 (4) GDPR.

In addition, where you plan to further process the personal data for a purpose other than the one for which the personal data were **initially collected**, firstly you must ensure that the further processing is **compatible** with the original purposes. In order to do so you must

²⁹¹ Guidelines on Automated individual decision-making and profiling, for the purposes of Regulation 2016/679, pg. 29.

²⁹² Art. 13 (2) (f), Art. 14 (2) (g) General Data Protection Regulation.

²⁹³ Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, as last Revised and Adopted on 6 February 2018, p.26.

assess the elements stated in Art. 6 (4) GDPR (such as, the link between the initial and further purpose, the context of the personal data, the nature of the personal data, etc.)

If the further processing is indeed compatible, then prior to the further processing, you must inform the data subject on the purpose and any other relevant information that changes due to the additional purpose of processing. Additionally, according to the Article 29 Working Party, you must provide further information on the **compatibility** analysis carried out (and as stated above). In this way, you give the opportunity to the data subject to consider the compatibility of the further processing and decide whether they want to exercise their rights (e.g., the right to restriction of processing or the right to object to processing).²⁹⁴ The point is that the data subject should reasonably expect that at the time and in the context of the collection of personal data a processing for a particular purpose may take place.²⁹⁵ Examples of further processing may be for scientific or historical research purposes or statistical purposes.

You can also use the Information Commissioner's Office guide on purpose limitation in order to guide you in the above assessment, which can be found [here](#).

13. If the personal data is collected from third-parties, or in another way other than directly from the data subject - is the source of collection of the personal data specified in the information notice?

- ☐ Yes, this information is provided
- ☐ No, this information is missed
- ☐ Not applicable (the data is collected directly from the data subject)

Where the respondent picked the negative answer, the below recommendation would come up.

It is recommended to integrate the information notice with this information, essential according to Article 14 (2) (f) GDPR.

Seeing as the data subject has not directly given out their personal data to you, the information notice will need to specify from which source the personal data originates, and if applicable, whether it came from publicly accessible sources.²⁹⁶

14. Does the information notice mention the existence of the right to request from the controller access to and rectification, or erasure of personal data, or restriction of processing concerning the data subject, or to object to processing, as well as the right to data portability and the right to withdraw consent, where applicable?

- ☐ Yes, this information is provided
- ☐ No, this information is missed

Where the respondent picked the negative answer, the below recommendation would come up.

The data subject must clearly be informed about their rights under the GDPR, including the²⁹⁷:

- right to obtain a confirmation from the controller of the personal data concerning him or her that are being processed, **and** access that personal data;
- right to rectify or erase their personal data without undue delay;
- right to restrict the processing of their personal data where the personal data is inaccurate or the processing is unlawful, or the controller no longer needs the personal data for the purpose(s) of the processing;

²⁹⁴ Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679, as last Revised and Adopted on 11 April 2018, p.24.

²⁹⁵ Recitals 47 and 50 General Data Protection Regulation.

²⁹⁶ Art. 14 (2) (f) General Data Protection Regulation.

²⁹⁷ Art. 13 (2) (b), (c), (d) and Art. 14 (2) (c), (d), (e) General Data Protection Regulation.

- right to object, at any time, when the processing of their personal is based on the legitimate interest of the controller, **or** on the performance of a task carried out in the public interest;
- right to data portability in a structured, commonly used and machine-readable format
- right to lodge a complaint with a supervisory authority;
- right to withdraw their consent, at any time, if the legal basis used by the organisation is consent (or explicit consent).

The GDPR does not only require for the correct **elements** (as found in the questions above) to be included in the information notices, but also for the **way** it is communicated to be transparent. In a recent investigation by the French Data Protection Authority (“CNIL”) the tech giant Google LLC got fined 50 million euros for **lack of transparency**, and **inadequate information** due to the excessive multi-layered approach they took in providing information. This goes to show that in order to follow the GDPR **principle of transparency** a controller must ensure to have an effective means of providing information to the data subject.²⁹⁸ If you want to find out your compatibility with it, answer the following questions.

15. Is the information notice concise, transparent, intelligible and easily accessible?

- ☐ Yes
☐ No

Where the respondent picked the negative answer, the below recommendation would come up.

The information must be presented in an efficient manner (“concise and transparent”), in order to avoid information fatigue. For this reason, the privacy policy should be differentiated from other non-privacy related information (i.e., contractual provisions or general terms of use). In the cases where the information notice is provided online, it is also possible to use a layered approach, which will allow the data subject to navigate to particular sections that may be of interest to them without having to read the whole text. The Guidelines on Transparency by the Working Party 29 state that the information should be understood by an average member of the intended audience (“intelligible”) – meaning that you may need to try different mechanisms to find the most appropriate manner of presenting the information. Lastly, the information notice should be able immediately apparent to the data subject, for example, providing it directly to them, linking them to it, or having it appear in Frequently Asked Questions (FAQs).

16. Is the information notice written in clear and plain language?

- ☐ Yes
☐ No

Where the respondent picked the negative answer, the below recommendation would come up.

You should aim to provide the information in as simple a manner as possible, without including complex sentences and legal language. Furthermore, the information should be concrete, not leaving any space for doubts or misunderstandings or other interpretations by the data subjects.²⁹⁹ It is especially important that the purposes and the legal basis for the processing is clear. Please keep in mind that the requirement for clear and plain language is even more important when the information is provided to children, therefore the vocabulary, tone, and style of the language should be adapted so that the children understand the information that is being presented to them.³⁰⁰

²⁹⁸ Guidelines on Transparency under Regulation 2016/679, as last Revised and Adopted on 11 April 2018.

²⁹⁹ Guidelines on Transparency under Regulation 2016/679, as last Revised and Adopted on 11 April 2018, p.6.

³⁰⁰ Article 12(1) General Data Protection Regulation.

17. Is the information notice provided free of charge?

☐ Yes

☐ No

As a data controller, you cannot charge data subjects simply for providing them information in a general manner; or in a way that seems as a condition for the purchase of services or goods.³⁰¹

³⁰¹ Guidelines on Transparency under Regulation 2016/679, as last Revised and Adopted on 11 April 2018, p.6.

ANNEX C. PRESENTATION SLIDES FOR GDPR WEBINAR

cyberwatching.eu
The European watch on cybersecurity & privacy

Interactive Webinar on the
20th July 2021

GDPR TEMPERATURE TOOL

Anastasia Botsi, Associate – ICT Legal Consulting International

ICT LEGAL CONSULTING

www.cyberwatching.eu
[@cyberwatching.eu](https://twitter.com/cyberwatching.eu)
info@cyberwatching.eu

Funded by the European Commission
Horizon 2020 – Grant # 740129

2

cyberwatching.eu
The European watch on cybersecurity & privacy

The European watch on Cybersecurity and Privacy

- Map, cluster and collaborate EU Research & Innovation**
+175 EU projects
- EU Project Hub** Simple and collaborative platform for EU-funded cybersecurity and privacy projects. Cooperation and Cluster workshops to foster collaboration and market readiness of results.
- Promote EU innovation to the EU market**
+50 startups series
- Marketplace** A central Marketplace of R&D results and services offered by projects across Europe. Market machines training for projects and SMEs. Free tools, guides and workshops for SMEs across the EU.
- Recommend policy and standards best practices**
+5 challenges for policy makers

3

cyberwatching.eu
The European watch on cybersecurity & privacy

The GDPR Temperature Tool
Improving the GDPR compliance posture of SMEs

A free online tool helping small businesses understand their risk of GDPR-related sanctions

Visit cyberwatching.eu | Download your customised action plan

20 Questions | 15 Minutes of your time | 1 Recommendations report

Answer the GDPR-sanction related questions | Act and implement change in your organisation

*The GDPR sanction tool is not an attorney fee. It is a tool to help you understand the risk assessment that should be conducted by SMEs. Please do not rely on the results of this tool as a basis for your processing activities.

Cyberwatching.eu presentation May 2017 | www.cyberwatching.eu | @cyberwatching.eu

4

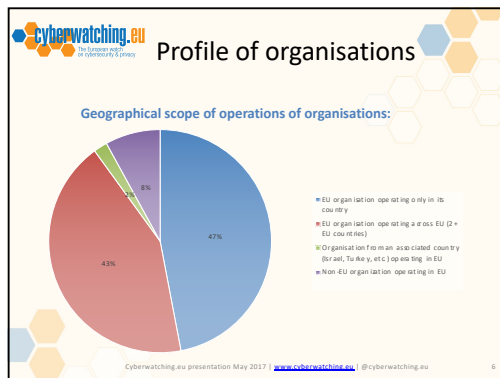
cyberwatching.eu
The European watch on cybersecurity & privacy

Agenda

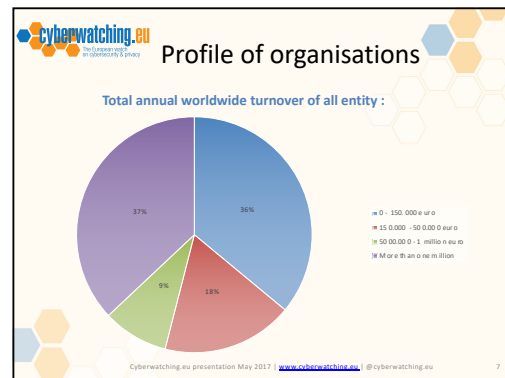
- Results of the responses of the GDPR Temperature Tool
- Analysis of the main gaps emerged during the compilation of the questionnaire
- Further insights on the recommendations given based on the obligations described in the questionnaire
- Interactive session of Q & A on aspects of GDPR compliance
- Feedback on GDPR Temperature Tool

Cyberwatching.eu presentation May 2017 | www.cyberwatching.eu | @cyberwatching.eu

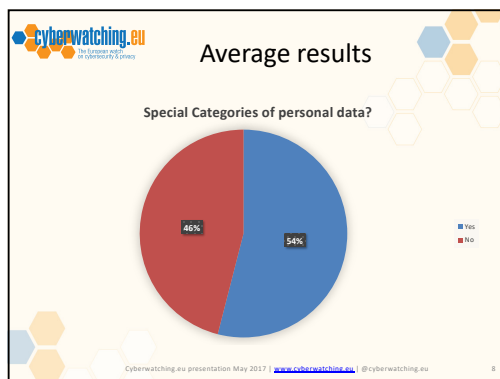
5



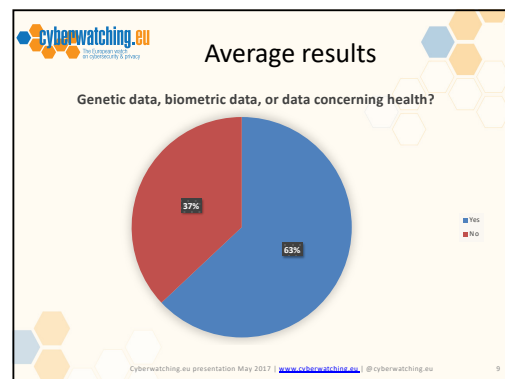
6



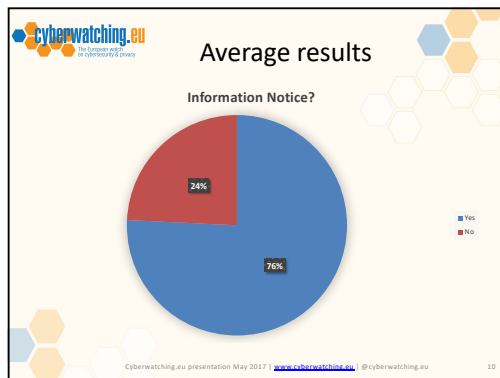
7



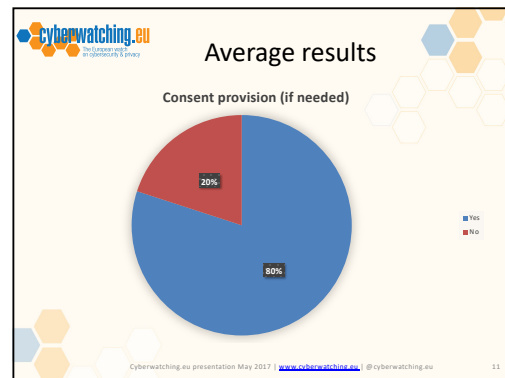
8



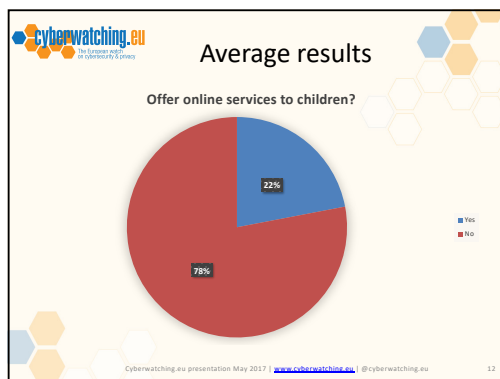
9



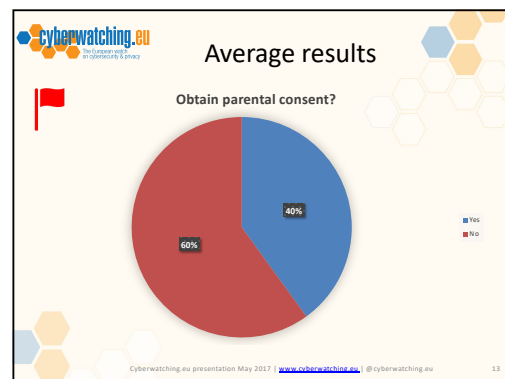
10



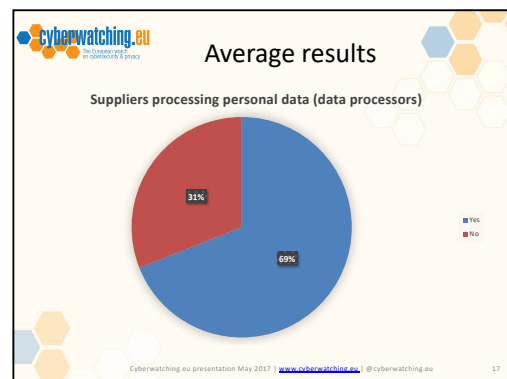
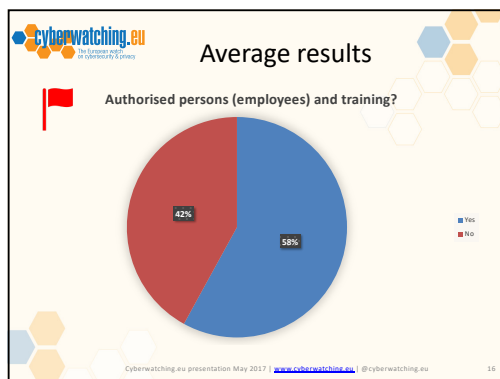
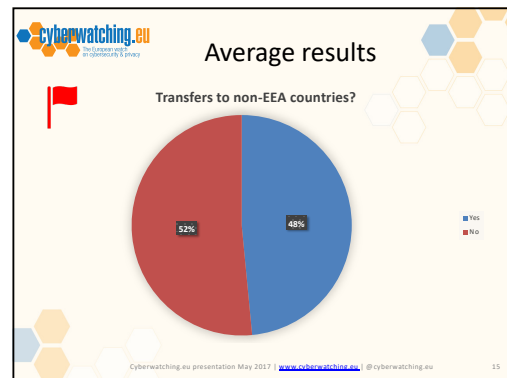
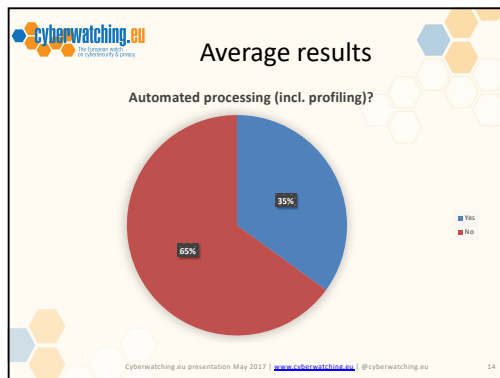
11

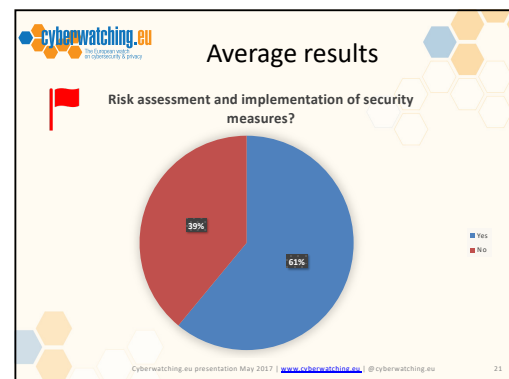
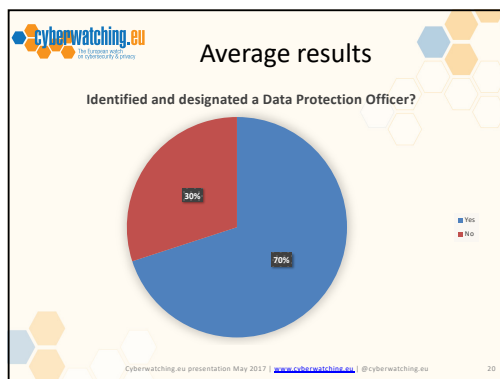
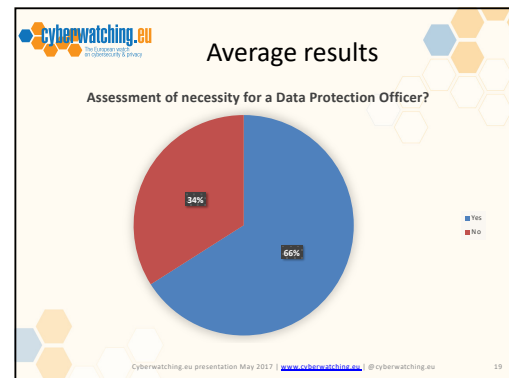
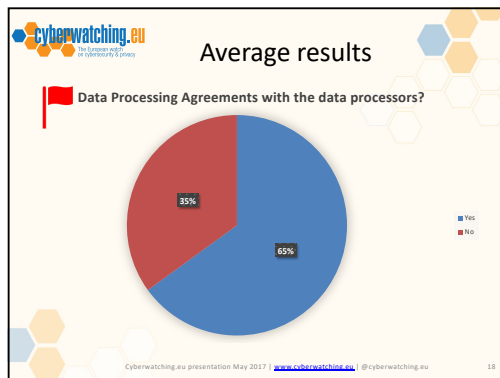


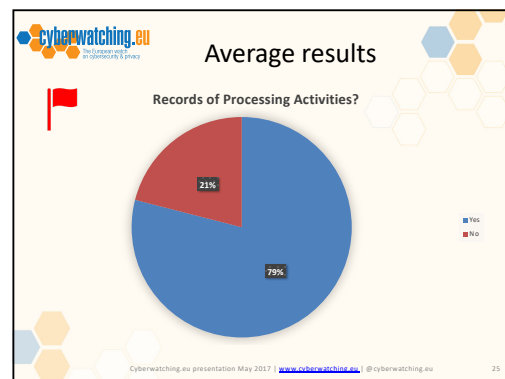
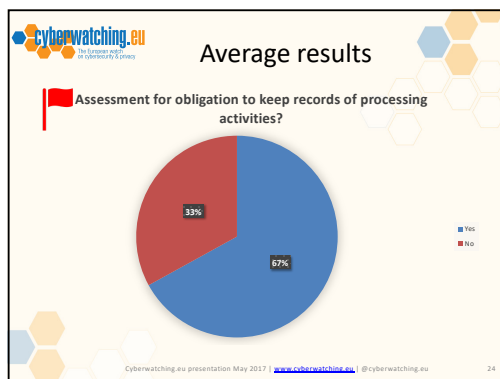
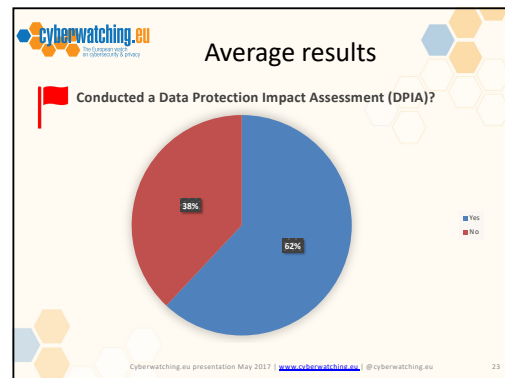
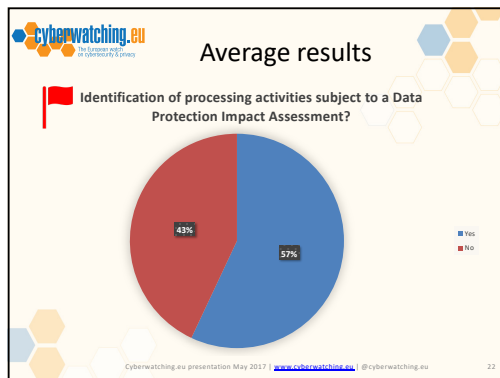
12

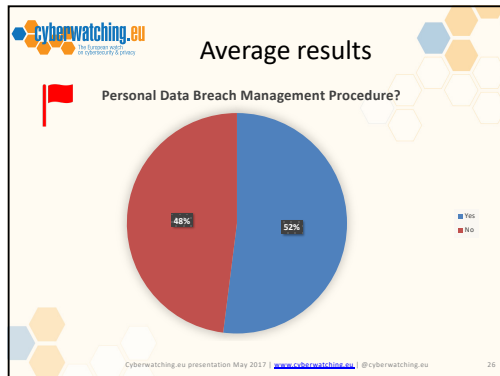


13

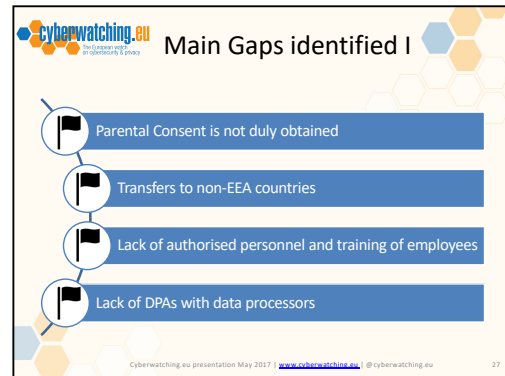




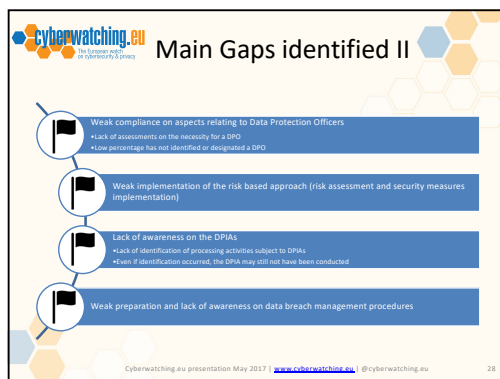




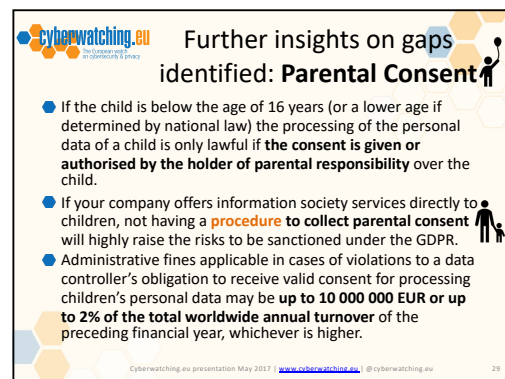
26



27



28



29

cyberwatching.eu the European agency for cybersecurity & privacy

Actions to obtain parental consent

- Check the age which requires parental consent for each Member State(s) where your company offers information society services to children
- Obtain consent by establishing the age of the child with a **level of certainty** appropriate to the risks that arise from your data processing ([ICO Code of Practice for age-appropriate design for online services](#))
 - Self-declaration (user states age with no evidence – low risk operations – low certainty)
 - Artificial Intelligence (estimate user's age based on interactions with service or check consistency with self-declared age – greater certainty)
 - Inform users prior to processing
 - Collect the minimum amount of personal data for this purposes
 - Not use any personal data for other purposes

Cyberwatching.eu presentation May 2017 | www.cyberwatching.eu | @cyberwatching.eu 30

30

cyberwatching.eu the European agency for cybersecurity & privacy

Actions to obtain parental consent

- Obtain consent by establishing the age of the child with a **level of certainty** appropriate to the risks that arise from your data processing ([ICO Code of Practice for age-appropriate design for online services](#))
 - Third party age verification services (assurance of user's age based on 'attribute' system)
 - Due diligence checks to ensure level of certainty with which it confirms age is sufficient (PAS standard 1296 'Online age checking')
 - Inform users prior to processing
 - Account holder information (existing adult account holder for logged-in or subscription-based services)
 - Hard identifiers (solutions that link back to formal identity documents, i.e. passport)
 - Avoid providing only this choice, unless the risks inherent to the processing warrant such approach
- Implement **technical measures discouraging false declarations** of age, or identify and close underage accounts to strengthen self-declaration mechanisms (e.g., prevent user from resubmitting immediately)

Cyberwatching.eu presentation May 2017 | www.cyberwatching.eu | @cyberwatching.eu 31

31

cyberwatching.eu the European agency for cybersecurity & privacy

Further insights on: data transfers

On July 2020, in the so-called **Privacy Shield** case, the Court of Justice of European Union (CJEU) invalidated the EU-US Privacy Shield and, although upheld the validity of the Standard Contractual Clauses (SCCs) it put forth important requirements for controllers when using the SCCs (obligation to assess the level of protection of the third country).

On 4th June 2021, the European Commission published the final Implementing Decision to adopt the new / modernized **Standard Contractual Clauses**.

On 18th June 2021, the European Data Protection Board (EDPB) adopted the final version of **Guidelines on the implementation of the SCCs** to ensure compliance with the EU level of protection of personal data, which were first adopted in November 2020 after the Schrems II ruling.

Cyberwatching.eu presentation May 2017 | www.cyberwatching.eu | @cyberwatching.eu 32

32

cyberwatching.eu the European agency for cybersecurity & privacy

3 aspects of the Schrems II ruling

- The EU-US Privacy Shield held to be invalid**
The Court found that the local (US) laws did not satisfy the 'essential equivalence' requirement that EU data protection law guarantees (e.g., surveillance programs enabling access by public authorities to EU citizens' personal data for security purposes).
- Standard Contractual Clauses held to be valid – with qualifications to ensure adequate data protection**
Noting that if the SCCs are the basis of data transfers in a third country, the level of protection must be 'essentially equivalent' to the level of protection guaranteed under the GDPR. The third countries' level of protection has to be assessed by the data exporter taking into consideration the legal system of the jurisdiction where the data would be transferred.
- The active role of Supervisory Authorities in regulating data transfers through SCCs**
The Court clarifies that Data Protection Authorities must take appropriate actions to remedy inadequacies in the SCCs or its enforcement (including transfer suspensions or prohibitions).

For more info, see also the [FAQ on the Schrems II decision](#) published by the EDPB.

Cyberwatching.eu presentation May 2017 | www.cyberwatching.eu | @cyberwatching.eu 33

33


Relevant decisions post-Schrems II: Mailchimp (Bavarian DPA)

- In March 2021, the Bavarian DPA determined that the use of the newsletter tool Mailchimp by a German company was unlawful.
- The transfer of email addresses to the US was based on the SCCs and the company had not considered whether "additional measures" were necessary in addition to SCCs.
- Mailchimp may in principle be subject to data access by US intelligence services as an Electronic Communications Service Provider. Therefore "the transfer could only be lawful if such additional measures (if possible and sufficient to remediate the problem) were taken."
- As the respondent declared to refrain from using Mailchimp with immediate effect, the DPA did not impose a fine or a formal declaratory decision.

More info on the decision is available [here](#).

34

Relevant decisions Post-Schrems II: INE (Portuguese DPA)




- On 27th April 2021, the Portuguese DPA (CNPD) ordered the Portuguese Statistics Institute, INE, under Art. 58(2)(j) GDPR, to suspend the transfer of Census 2021 data to the USA and other third countries which have not received an adequacy decision, through Cloudflare or any other service provider, within 12 hours.
- INE must also ensure that any other processors engaged are not bound by local laws which may lead to conflicts with the GDPR's obligations.
- The CNPD received more than 10 complaints about the Portuguese Statistics Institute (INE)'s Census 2021 initiative, through which the INE carries out a periodic census of the Portuguese population. Some of these complaints suggested that submitted personal data might be transferred to a company located in the USA.
- The data included personal data and sensitive data (health and religion data)

More info on the decision is available [here](#).

35

EDPB Roadmap for data transfers




**Step 1 :
Know your transfers**

1. Identify the transfers of personal data outside the EEA and verify the corresponding transfer mechanisms that you will rely on
 - recording, mapping and understanding (sub) processors
 - Understanding further or onward transfers
 - Remove access from a third country or cloud storage in a cloud situated outside the EEA is also a transfer!

36

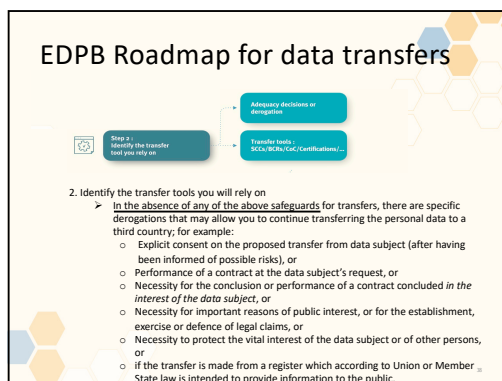
EDPB Roadmap for data transfers



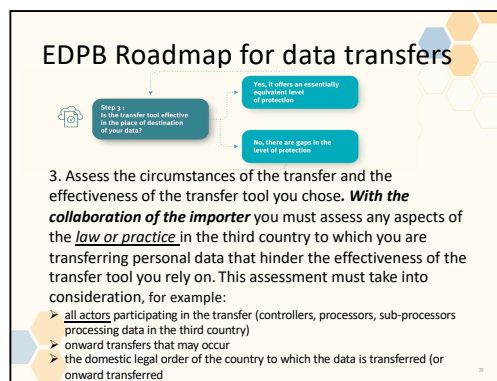
2. Identify the transfer tools you will rely on
 - Check the adequacy decisions [here](#)
 - If absence of adequacy decision you must consider the transfer tools of:
 - Standard data protection clauses adopted by the Commission, which are probably the most common way of transferring personal data outside the European and are stipulated in [Article 46 GDPR](#).
 - Codes of conduct, approved by the competent supervisory authority (May 19th 2021 the Belgian Supervisory Authority [approved](#) the first transnational code of conduct adopted within the EU since the GDPR entered into force, the [EU Data Protection Code of Conduct for Cloud Service Providers](#).)
 - Certification mechanisms, approved by the competent supervisory authority
 - Binding Corporate Rules

In the absence of any of the above safeguards for transfers, there are specific

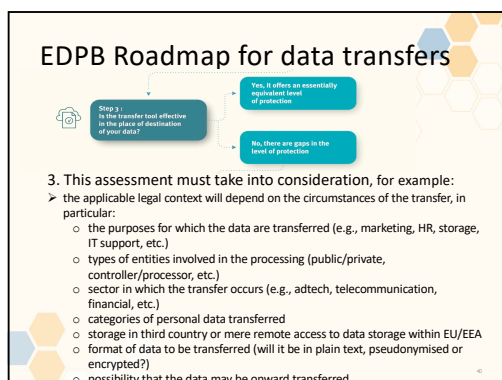
37



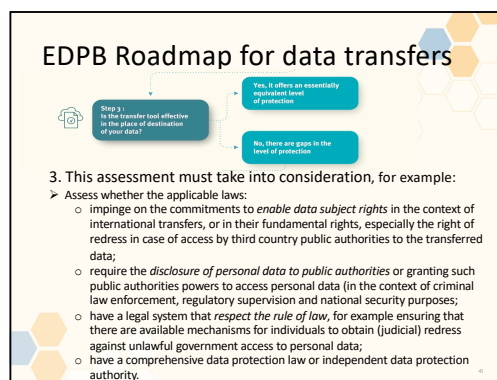
38



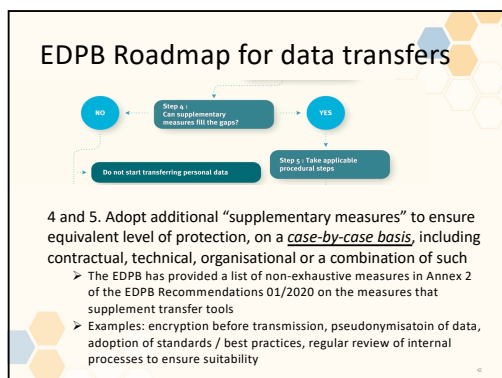
39



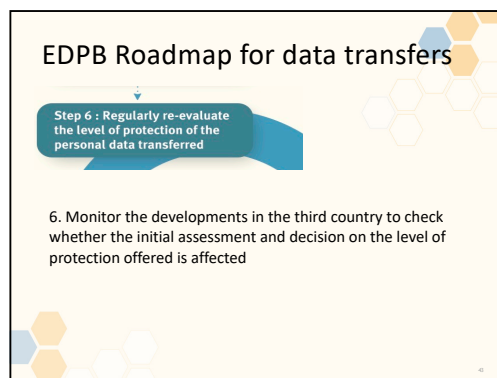
40



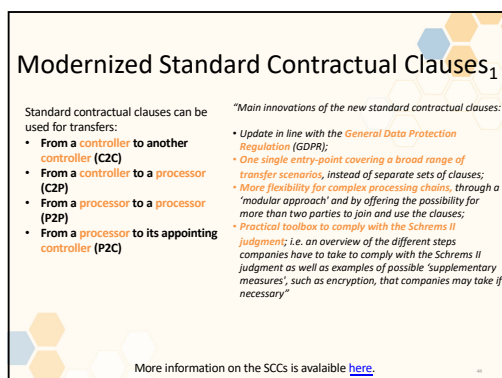
41



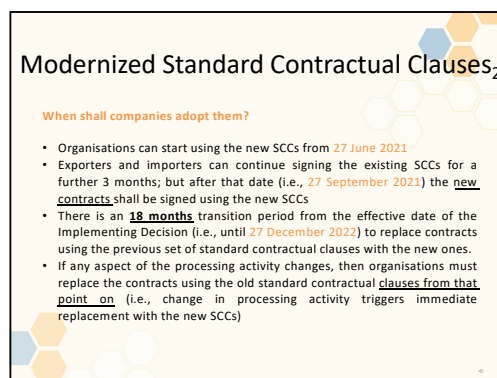
42



43



44



45

What to do as data exporters?

- ✓ **Identify transfers** to the US (e.g., using your Records of Processing Activity) and more generally to non-EU countries.
- ✓ **Verify the legal basis:**
 - If you relied on the Privacy Shield, you need to identify a **new legal basis**, e.g., SCCs or, if applicable, one of the derogations of Art. 49 GDPR, e.g., data transfer necessary for the performance of a contract to which the data subject is party;
 - If you rely on the Standard Contractual Clauses, you still need to perform a **Data Transfer Impact Assessment** and it may be necessary to proceed to the assessment and implementation of "supplementary measures" which can be of contractual, technical or organisational nature – see Annex 2 (GDPR Recommendations 01/2020)
- ✓ **Contact suppliers (data processors) proactively**, to indicate that, if the processing entrusted to them involves, either directly or by means of sub-providers (sub-processors), transfers to the US or to other third countries that do not permit effective compliance with the EU core principles, it will be necessary to proceed to the **identification of a legal basis** such as, for example, the new SCCs (or, where applicable, one of the derogations under Article 49 GDPR, e.g., transfer of data necessary for the performance of a contract to which the data subject is a party) and **assess the application of "supplementary measures"** (after performing a **Data transfer Impact Assessment**)
- ✓ Once the reorganization of transfers to non-EU countries has been completed, **consistently modify the Record of Processing Activities** (art. 30 GDPR) and the information provided pursuant to articles 13-14 GDPR;
- ✓ **Verify and consistently modify references to the Privacy Shield in your privacy documentation** (e.g., privacy policies, procedures, contracts, etc.);
- ✓ **Closely monitor the activities of the relevant supervisory authorities** regarding further interpretations and practical advice to bring any non-EU transfers into line with the Schrems II decision and more generally with applicable data protection legislation.

46

Data Transfer Impact Assessment

- The data exporter, even when using the SCCs, has to carry out a **Data Transfer Impact Assessment** ("DTIA"), to evaluate the level of data protection guaranteed by the third country; then, the data exporter shall assess the need for **supplementary measures**, in addition to the SCCs, in order to guarantee an adequate level of protection.
- The DTIA has to be **documented** and be **made available** on request of the competent supervisor **authority**
- Clause 14 (b) of the SCCs describes elements to consider while making this assessment:
 - i) the **specific circumstances of the transfer**, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
 - ii) the **laws and practices of the third country of destination**—including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
 - iii) **any relevant contractual, technical or organisational safeguards** put in place to supplement the safeguards under the SCC, including measures applied during transmission and to the processing of the personal data in the country of destination.

47

Further insights on: Authorised Persons

- **Internal company alignment** with the expectations and obligations each employee is integral to lowering a company's risk to compliance (Raise attention to data protection in the entire company structure, from high level management to the employees or even candidates prior to hire).
- **Actions to take:**
 - Short written instructions to employees when they are onboarding the company, including their **responsibilities** when processing personal data, as well as the necessary precautions they should take when doing their job.
 - Designate "persons authorised" to process personal data, for example, those employees that are constantly processing personal data.
 - Train "persons authorised" to make them aware of the main risks that the processing operations may pose to the protection of the personal data.
 - Demonstrate training to the outer world, by for example, organising annual training sessions
 - **Keeping records** of the participants of the training.

Cyberwatching.eu presentation May 2017 | www.cyberwatching.eu | @cyberwatching.eu

48

Further insights on: Data Processing Agreements with Processors

- Data controllers are responsible for the personal data they collect and process – as well as the data that is processed by your chosen data processors. Not having entered into any form of contractual agreements with your processors increases your exposure to sanctions of the GDPR.
- **Actions to take:**
 - The Data Processing Agreement, must at least include: the subject-matter and duration of the processing; the nature and purpose of the processing; the type of personal data; the categories of data subjects; the obligations and rights of the data controller against the data processor.
 - Organised archive of the signed DPAs between you and your suppliers or service providers as data processors
- Useful resource on this is the **template for a Data Processing Agreement** by the gdpr.eu project which you can complete and enhance, where necessary, with the details of the nature and purpose of the processing, as well as the type of personal data and categories of data subjects.

Cyberwatching.eu presentation May 2017 | www.cyberwatching.eu | @cyberwatching.eu

49

cyberwatching.eu
The European web
in cybersecurity & privacy

Further insights on: Risk Assessments and Security Measures

- The risk-based approach that the GDPR has implemented requires all companies evaluate what the risk of each processing activity is, before the processing activity is carried out – that way the company can implement the appropriate technical and organisational measures to ensure a level of security **appropriate to the risk**. The important note for the evaluation of the risk is not only that it indeed occurs but that the company is also able to demonstrate that it has occurred.
- Actions to take:**
 - Conduct a risk assessment to map your processing activities.
 - Drafting a document that describes how the risk assessments are done, to show the logic in cases of investigations.
 - Create an internal document that describes the security measures that are implemented depending on the risk of the processing activity (also useful for demonstrating to processors the security standards you expect from them).
- Resources and tools:** ENISA's customizable online tools for the security of personal data processing.
- ENISA's risk assessment tool** for carrying out risk assessments guides SMEs through their specific data processing activities and helps you evaluate the relevant security risks. This tool builds on the existing tools that exist, such as the [CNIL's methodology for assessing risk management](#), ENISA's [recommendations for a methodology of the assessment of severity of personal data breaches](#), and ENISA's [Risk Management and Risk Assessment for SMEs](#) pilot study.
- ENISA's self assessment of the implemented security measures**, helps to assess the risk level for a given processing activity and the appropriate security measures taken. This secondary tool can be used as a method of identifying whether the security measures are adequate and to check the status of their implementation.
- An [online tool](#) for cybersecurity in hospitals produced by ENISA. The aim is to help healthcare organisations to quickly identify the most relevant guidelines (such as assets processed or related threats) and promote the importance of a good procurement process to ensure appropriate security measures.

Cyberwatching.eu presentation May 2017 | www.cyberwatching.eu | @cyberwatching.eu 50

50

cyberwatching.eu
The European web
in cybersecurity & privacy

Further insights on: Risk Assessments and Security Measures

- Security tools and solutions can also be found in the Cyberwatching.eu marketplace, which can increase the level of compliance with the GDPR, of SMEs or other companies.
- CYBERWATCHING**, is a Secure Cloud Identity Wallet, which provides end-to-end secure and privacy-preserving platform for managing and storing users' digital identity information, ranging from authentication credentials over medical reports to tax data or similar. This solution uses cryptographic mechanisms, as well as determining which of their data goes where. If your SME involves data sharing services, this software may be leveraged as a way to extend your portfolio with privacy enhanced and authenticity.
- WITCOM's data masking** component can be utilised as a security measures for sharing data or for storing data in non-trusted environments.
- The **PRISM project** provides an innovative data privacy governance platform which supports **healthcare** organizations towards GDPR compliance using advanced modelling languages and methodologies for privacy-by-design and data protection management. Specific innovations of the project include: the development of advanced modelling languages and methodologies for **privacy-by-design** and **data protection management**; automated methods and techniques to elicit, map and analyse data that organizations hold for individuals; **integrated encryption and anonymisation solutions** for GDPR; methods and automation techniques for the specification, management and enforcement of personal data consent; a modular solution that covers different aspects of GDPR.
- The **PANACEA project** has developed, with three European Healthcare Centres, a people-centric toolkit of innovations to **assess and improve the cybersecurity readiness of healthcare socio-technical systems** (I.T. networked medical devices, staff) and of medical device/system lifecycles.
- SAVEDATA project** (Secure Data sharing platform) provides technical tools to ensure compliance with the EU GDPR. **QUINIFON** integrates its data security components with Data Masking services to support only authorised access to the masking/unmasking services, and masked data.
- Avenue is an SME that provides professional solutions for the comprehensive management of IT infrastructure for companies and institutions and has a product called [AUSONITO](#).

Cyberwatching.eu presentation May 2017 | www.cyberwatching.eu | @cyberwatching.eu 51

51

cyberwatching.eu
The European web
in cybersecurity & privacy

Further insights on: Data Protection Impact Assessments

- A DPIA is necessary when a processing operation is **likely to result in a high risk** to the rights and freedoms of natural persons. This is particularly the case when **new technologies** are being introduced within your company. Other examples of a processing operation that is "likely to result in high risks" are:
 - An **automated processing** which uses a **systematic and extensive evaluation of personal aspects** relating to natural persons, including profiling, and on which decisions are based that **produce legal effects** (either to that natural person or significantly affect that person) (more details on what this entails can be found in question 8);
 - A processing of **special categories** of personal data, or a processing relating to **criminal convictions and offences on a large scale**;
 - A **systematic monitoring of a publicly accessible area on a large scale**.
- Actions to take:**
 - Rely on the French Data Protection Authority modular tool to conduct the assessment, through a step-by-step process, which can also be customised based on the specific needs of an SME or your business sector. (available in both portal and web versions, and can be found for free [here](#).)
 - Check whether your processing activities fall within the activities that must mandatorily carry out a DPIA in the Member States you are operating in, available [here](#) but also in the designated national supervisory authority's website.

Cyberwatching.eu presentation May 2017 | www.cyberwatching.eu | @cyberwatching.eu 52

52

cyberwatching.eu
The European web
in cybersecurity & privacy

Further insights on: Records of Processing Activities

- The GDPR stipulates the obligation that each controller and processor must maintain a record of processing activities. It is recommended that you keep this record updated regularly, according to the functional and practical evolving of data processing. In practice, if new data is collected, if the retention period is changed, or if a new processing recipient is involved, this must be added to the record.
- Resources, Tools & Solutions:**
 - A **template of the record of processing activities** has been developed by the Cypriot Office of the Commissioner for Personal Data Protection.
 - A **template of record of processing activities** which has been developed by the French Commission National Protection Authority (CNIL) that provides a template for both data controllers and data processors. Commission Nationale de l'Informatique et des Libertés, [Record of Processing Activities](#).

Cyberwatching.eu presentation May 2017 | www.cyberwatching.eu | @cyberwatching.eu 53

53

cyberwatching.eu Further insights on: **Personal Data Breach Management Procedure**

- The GDPR gives the timeline of notifying the supervisory authority of the data breach within 72 hours, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the data subjects. For these reasons you need to have protocol, or a procedure determined in order to recognise when a data breach has occurred, how it will be recognised, how the company will react to it, and who will be involved in these steps. The answers to the above questions will result to a procedure on data breach management.
- In defining a procedure on data breach management, we suggest taking into consideration the evaluation of the likelihood that the breach results in risk to the rights and freedoms of the data subjects by applying:
 - the accountability principle set forth in the GDPR in order to be able to demonstrate the responsiveness and actions taken as a result of a personal data breach to the supervisory authority, by at least documenting any personal data breaches and subsequent actions including: a) the facts relating to the personal data breach, b) its effects to data subjects and, c) the remedial action taken.
 - the methodology provided by the European Agency for Network and Information Security (ENISA) to assess the severity of personal data breaches by taking into account:
 - the data processing context, i.e., the type of data breached, and the overall processing operation,
 - the ease of identification of the data subjects from the data involved in the breach,
 - the specific circumstances of the breach, for example, whether it is a loss of confidentiality, or any malicious intent that may be involved.

Cyberwatching.eu presentation May 2017 | www.cyberwatching.eu | @cyberwatching.eu 54

54

cyberwatching.eu Further insights on: **Personal Data Breach Management Procedure**

- The data controller is also required to communicate a breach to the affected individuals, "when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons". The communication should be done as soon as possible (namely "without undue delay") and aims to provide individuals with specific information about the steps they should take to protect themselves. This could also be done by providing specific advice to individuals to protect themselves from adverse consequences of the breach (for instance, resetting passwords).
- Breaches should be communicated to the concerned individuals directly with dedicated and transparent methods of communication which can ensure individuals understand the information being provided to them (e.g., email, SMS or prominent website banners in relevant languages).
- Notification to individuals is not required when:
 - the controller has applied appropriate technical and organisational measures to protect personal data prior to the breach (such as state-of-art encryption);
 - immediately following a breach, the controller has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise;
 - it would involve disproportionate effort to contact individuals.
- Actions to take:
 - Keep track of any incidents that have occurred (even those that you have labelled as not personal data breaches) and the mitigating actions taken or notifications sent to the supervisory authority or data subjects, through for a register of personal data breaches.
 - Harmonise and possibly integrate the data breach procedure with any eventual cybersecurity incident handling procedure.
 - Consider useful tools and solutions that can help you prevent, detect and mitigate personal data breaches

Cyberwatching.eu presentation May 2017 | www.cyberwatching.eu | @cyberwatching.eu 55

55

cyberwatching.eu Further insights on: **Personal Data Breach Management Procedure**

- Resources, Tools & Solutions:**
 - Self assessment checklist for GDPR Readiness Checklist Tool on legal basis (click on "data security") by the Irish Data Protection Commission.
 - The Data breach notification tool developed by the Italian Garante.
 - Fitsec Ltd is a Finnish cyber security company that offers cybersecurity services, including the Asset tracker which can be found in Cyberwatching.eu's Marketplace. The Asset tracker assists organisations in detecting their data leaks. Specifically, this service enables them to track personal data of an organisation and check if the data has leaked to the internet. The service is easy to use and does not require any installations in your environment. From the easy-to-use web interface, you can see the assets being monitored, add new assets to be monitored and analyse any matches that have been found. All findings are reported to you in whatever way you desire.
 - GuardDns is an automated compromise assessment platform developed by an SME, which can act as a preventative - bird-eye vision of the network. However, there would need to be another system in place in order to ensure that the personal data breach is detected as soon as possible and communicated to the supervisory authority or the data subjects (should there be a high risk to the data subject) within 72 hours.

Cyberwatching.eu presentation May 2017 | www.cyberwatching.eu | @cyberwatching.eu 56

56

cyberwatching.eu Q&A / Feedback on Tool

- Feel free to ask any questions on the above!
- Please take a minute to fill out the Feedback Form [here](#):

Did you find this tool easy to use and clearly understandable? *

☐ Very easy
☐ Easy
☐ Not easy

How likely is it for your organisation to use the recommendations, tools or solutions that we suggested? *

☐ Very likely
☐ Likely
☐ Not likely

Was the tool effective in helping you understand your compliance posture, and the aspects you need to further assess or work on to achieve a better level of compliance? (Fitness for purpose) *

☐ Very helpful
☐ Helpful
☐ Not helpful

Are there any data protection aspects which you need further support on? How can this tool be improved in order to better meet the needs of SMEs?

Cyberwatching.eu presentation May 2017 | www.cyberwatching.eu | @cyberwatching.eu 57

57



58

ANNEX D. PARTICIPATION AT LEGAL COMPLIANCE WEBINARS, WORKSHOPS, ROUND-TABLE DISCUSSIONS, PANELS

25/10/2017	Digital SME Workshop in León - Bridging R&I with the Business World ³⁰²
15/06/2018	Webinar on GDPR for SMEs - GDPR and SMEs: A practical look at the main duties and obligations and how to comply with them ³⁰³
05/9/2018	Webinar on Cybersecurity standards and certifications – the challenges - GDPR: the possible value of certification in data protection compliance and accountability ³⁰⁴
08/10/2018	ENISA workshop on Security of Personal Data Processing: Panel discussion – SMEs preparation for GDPR ³⁰⁵
10/10/2018	European Cybersecurity Forum: GDPR and recent EU directives and laws ³⁰⁶
10/12/2018	Digital SME Webinar on Privacy and Trust: Legal tips and compliance requirements ³⁰⁷
28/03/2019	H2020 Project clustering Workshop in Athens by the GHOST project - Legal Aspects: the GDPR & IoT ³⁰⁸
17/07/2019	Webinar on GDPR Compliance in the Age of Emerging Technologies ³⁰⁹
26/09/2019	Webinar on Cybersecurity for Healthcare: Human And Legal Perspectives: A Novices Guide to build a solid GDPR Data Protection Framework: a focus on the healthcare sector ³¹⁰
19/11/2019	Webinar on Blockchain: Multi-Application Viewpoints and Opportunities: Legal Aspects of Blockchain Technology: GDPR and its implications on Blockchain Technology ³¹¹
11/12/2019	Webinar on the Cyber Security Challenges in the IoT Era – Legal Aspects: The GDPR & IoT ³¹²

³⁰² Event information can be found here <https://www.digitalsme.eu/event-cybersecurity-bridging-ri-business-world-leon-spain-25-october-2017/>.

³⁰³ Event information and the PowerPoints can be found here <https://www.cyberwatching.eu/gdpr-smes>.

³⁰⁴ Event information and the PowerPoints can be found here <https://www.cyberwatching.eu/free-webinar-cybersecurity-standards-and-certification-challenges>.

³⁰⁵ The event report can be found here <https://www.enisa.europa.eu/events/personal-data-security/security-of-personal-data-processing-event-october-8-2018-notes>.

³⁰⁶ Event information can be found here <https://2018.cybersecforum.eu/en/krakow/>.

³⁰⁷ Event information and the PowerPoints can be found here <https://www.digitalsme.eu/webinar-privacy-trust-how-to-ensure-management-and-control-of-identities-and-rights/>.

³⁰⁸ Event information can be found here <https://www.cyberwatching.eu/news-events/events/h2020-project-clustering-workshop>.

³⁰⁹ The events' PowerPoint can be found here https://cyberwatching.eu/sites/default/files/Cyberwatching_GDPR-Webinar_Introduction%20-%20Nicholas%20Ferguson%20%2B%20Anastasia%20Botsi.pdf.

³¹⁰ Event information, a recording of the webinar and the PowerPoints can be found here <https://cyberwatching.eu/cybersecurity-healthcare-human-and-legal-perspectives>.

³¹¹ Event information, a recording of the webinar and the PowerPoints can be found here <https://cyberwatching.eu/blockchain-multi-application-viewpoints-and-opportunities/>.

³¹² Event information, a recording of the webinar and the PowerPoints can be found here <https://www.cyberwatching.eu/cyber-security-challenges-iot-era>.

22/10/2020	CharloT's workshop - Legal Aspects: the GDPR and IoT ³¹³
09/11/2020	Final conference of the Biocyber project: A Novices Guide to build a solid GDPR Data Protection Framework: a focus on the healthcare sector ³¹⁴
25/11/2020	DG Connect Roundtable for ICT Verticals and Horizontals for Blockchain Standardisation, 'Digital Society, Identity and Privacy': Legal Aspects of Blockchain Technology: Smart Contracts, Intellectual Property & Data Protection
10/12/2020	Webinar on Security and Privacy by Design for Healthcare: The Roadmap to GDPR Compliance in e-Healthcare services ³¹⁵
14/12/2020	Critical Chains workshop on Financial Sector Infrastructure Cyber-Physical Security and Regulatory Standards Workshop: Artificial Intelligence, Data Protection & Cybersecurity in the Fintech Sector ³¹⁶
16/02/2021	Webinar on The Data Governance Act and Data-Driven Policy Making: Impact and Practical Implementations ³¹⁷
10/05/2021	Digital SME Webinar on ePrivacy Regulation – What's the impact on SMEs?: ePrivacy regulation and the current data protection legal framework ³¹⁸
30/06/2021	Digital SME Webinar on Schrems II & Data Transfers – Decision & Impact on SMEs ³¹⁹
13/07/2021	Shaping the future of cybersecurity - Priorities, challenges and funding opportunities for a more resilient Europe: Privacy challenges and emerging technologies (AI, IoT, Blockchain) and how the R&I community is addressing them ³²⁰
20/07/2021	Interactive webinar on the GDPR Temperature Tool

Table 2 Legal compliance webinars, workshops, roundtables discussions, panels

³¹³ Event information and the PowerPoints can be found here

<https://www.chariotproject.eu/event/chariot-workshop/>.

³¹⁴ Event information can be found here

https://www.aeciberseguridad.es/index.php/Final_conference_of_the_BioCyber_project.

³¹⁵ Event information, a recording of the webinar and the PowerPoints can be found here

<https://www.cyberwatching.eu/security-and-privacy-design-healthcare>.

³¹⁶ Event information can be found here <https://cyberwatching.eu/financial-sector-infrastructure-cyber-physical-security-and-regulatory-standards-workshop>.

³¹⁷ The post-webinar report can be found here:

https://cyberwatching.eu/sites/default/files/POLICY_CLOUD_DGA_Postwebinar_Report_Mar2021.pdf.

³¹⁸ Event information, a recording of the webinar and the PowerPoints can be found here

<https://www.digitalsme.eu/events/sme-workshop-on-eprivacy/>.

³¹⁹ Event information, a recording of the webinar and the PowerPoints can be found here

<https://www.digitalsme.eu/events/the-schrems-ii-and-data-transfer-decision-and-impact-on-smes/>.

³²⁰ Event information, a recording of the webinar and the PowerPoints can be found here

<https://cyberwatching.eu/news-events/events/shaping-future-cybersecurity-priorities-challenges-and-funding-opportunities-more-resilient-europe>.

ANNEX E. R&I SOLUTIONS INDEX

1. [SMOOTH GDPR](#)

The target of the SMOOTH R&I (GDPR Compliance Cloud Platform for Micro Enterprises) is micro and small business becoming GDPR-compliant. SMOOTH provides easy-to-use and affordable tools to assess the level of compliance of small businesses. On the one hand, SMOOTH created awareness of the importance of complying with the new legislation delivering a **practical, interactive handbook** tailored to guide microenterprises through the GDPR requirements.

This resulted in the GDPR Handbook - an online handbook for micro-enterprises, providing detailed guidance on: how GDPR affects companies' organisation and daily activities; what actions they must undertake to become compliant; how to navigate through the regulation.

The SMOOTH project has the handbook also in an **iOs app and android app**. Companies can get tailored support for their data management, ensure they are GDPR compliant and improve their business.

2. [DEFEND](#)

The Data Governance for Supporting GDPR (DEFEND) project provides an **innovative data privacy governance platform** which supports **healthcare organizations** towards GDPR compliance using advanced modelling languages and methodologies for privacy-by-design and data protection management. Specific innovations of the project include, for example, automated methods and techniques to elicit, map and analyse data that organizations hold for individuals; integrated encryption and anonymisation solutions for GDPR; methods and automation techniques for the specification, management and enforcement of personal data consent.

DEFEND makes significant contributions in increasing trust, confidence and transparency through its platform. DEFEND will also increase the use of privacy-by-design principles in ICT systems and services at different levels. At the (service/system) planning level, it provides tools and methods from the security and privacy requirements area that support elicitation, modelling and analysis of privacy concerns from the early stages of the service/system development process. At the operational level, it provides analysis techniques and tools that implement privacy-by-design specifications. Apart from the practical contributions, the project also makes significant contributions to the PbD state-of-the-art by extending work in the PbD methodologies to operate within the context of the GDPR.

The DEFEND project has a limited scope of GDPR compliance in healthcare organisations, especially when it comes to designing services and systems in a healthcare organisation, and implementing security measures according to data protection by design (art. 32 GDPR).

3. [PANACEA](#)

The Protection and Privacy of Hospital and Health Infrastructures with Smart Cyber Security and Cyber Threat Toolkit for Data and People (PANACEA) project has developed a people-centric toolkit comprised of nine tools, to **assess and improve the cybersecurity readiness of healthcare socio-technical systems** (ICT, networked medical devices, staff) and of **medical device/system lifecycles**. It includes software-based innovative tools:

- dynamic risk assessment, based on a multi-layer attack graph model including “human” and “business” layers, and automatic generation of mitigation recommendations,
- inter-organizational secure information and heavy images sharing,
- regulatory compliant security-by-design and certification of systems/medical devices,
- machine-to-machine and smartphone-based facial identification (also with masks).

These tools could be useful to demonstrate privacy by design, and the risk-based approach by the hospital and healthcare sector, as well as proposing security-by-design for systems and medical devices. In addition, the PANACEA platform can also increase business continuity and patients' trust, as well as reducing the risk of improper access to patients' related data.

The PANACEA platform also includes non-technical tools, influencing staff behaviour and supporting the management through contextualized risk governance models, educational voiceless videos, methodology to produce behavioural “nudges”, methodology to maximize cybersecurity return-on-investment, guidance for contextualized deployment of previous tools. These could be implemented as organizational measures by the healthcare sector to further enhance their security measures under article 32 GDPR.

As a result, the PANACEA project can help increase the cybersecurity compliance in the healthcare sector, including the implementation of security-by-design, the increase in preparedness and training of employees, and the protection of important existing systems/medical devices which were designed when cybersecurity was not a problem from healthcare organisations. Therefore, it is recommended for SMEs to rely on the tools created by the PANACEA project.

4. [PAPAYA](#)

The [PAPAYA project](#) is developing **privacy-by-design solutions** and a dedicated platform to address the privacy concerns when **data analytics tasks are performed by untrusted third-party data processors**. PAPAYA has designed and developed dedicated privacy preserving data analytics primitives that enable data owners to extract valuable information from protected data (encrypted data), while being cost-effective and accurate. There is a wide variety of innovations of the project include a Privacy Engine, Mobile usage statistics service, Mobile patterns analytics service; Threat detection for sensitive data service; Privacy-preserving Arrhythmia Classifier; Compliance tools; Privacy-preserving

analytics platform; Privacy-preserving data analytics modules; Privacy-preserving collaborative training of neural networks; Privacy-preserving training of neural networks.

The PAPAYA project allows for organisations to leverage the value of the data the organisations may collect or have collected, while at the same time applying security measures such as encryption. Based on the research, PAPAYA can help improve the way data analytics are carried out in order to ensure both an accurate result but also a transparent process for the data subjects. The project seems to be utilizing different privacy-preserving techniques in order to ensure that value is obtained from data analytics, but also that the privacy of individuals is respected.

5. [CREDENTIAL](#)

The CREDENTIAL project **targets cloud and identity providers** who want to extend their portfolio with **privacy enhanced and authentic data sharing services** by leveraging the CREDENTIAL software. On the other hand, CREDENTIAL can also be leveraged by service providers to learn how they can indirectly benefit from the CREDENTIAL Wallet service by registering as a receiving endpoint for authentic user data, thus providing more trustworthy eBusiness solutions.

CREDENTIAL Wallet demonstrates that if the users' data are stored in the CREDENTIAL Wallet, they are protected as a preventive measure by strong **cryptography** from the most common threats in cloud computing, even from the cloud provider itself. At the same time, data is easily accessible anywhere, anytime, and all communication devices without complex synchronization and configurations work. In essence, the project provides a versatile and easy-to-use solution to securely manage personal data in the cloud.

The result relevant for the compliance of service providers (through cryptography as a security measure according to article 32 GDPR) when it comes to sharing data and identity management is the [CREDENTIAL Wallet Platform](#). This platform is an all server-side and client-side components and apps needed for secure and privacy-friendly data sharing and identity management in the cloud. It is an open and flexible cloud identity wallet architecture to easily connect to other identity management systems.

6. [KRAKEN Project](#)

The KRAKEN project (Brokerage and market platform for personal data) aims to enable the sharing, brokerage, and trading of potentially sensitive personal data, by returning the control of this data to citizens (data providers) throughout the entire data lifecycle. KRAKEN aims to **standardize different IT solutions** by using **privacy-preserving** integration techniques of **independently obtained data sources from subjects consenting to different analyses**. The project combines, interoperates, and extends the best results from two existing mature **computing platforms** developed within two **H2020 actions: CREDENTIAL and MyHealthMyData**. Since no results have been produced yet by this project it is yet to be determined by future projects whether its results can help in the compliance efforts with the GDPR.

7. [SUNFISH platform](#)

The Secure Data sharing (SUNFISH) platform therefore focuses on enabling the sharing of data between potentially untrusted entities while protecting the sensitive data of each entity. This is achieved through several components for **controlled data sharing between services** provided by different private clouds, to be invoked when the mechanism they provide is the most efficient.

The SUNFISH platform has three pillars: **security by design, flexibility and decentralisation**. Blockchain is the corner stone of the solution and the key enabler to a fully the interaction between blockchain technology and the SUNFISH **FaaS – Federation-as-a-Service** – solution. The **Service Ledger** harnesses the power of **blockchain** and **smart contracts**, SUNFISH makes possible the creation of an innovative kind of **distributed governance without trust**. Such a solution can be flexibly adapted to the needs of participating clouds and partners in the federation by making use of existing identity-management components. The flexibility allows its users to collaborate and securely share their private cloud resources and it guarantees secure information sharing, provided by **dynamic data masking** as much as **secure multiparty computation**.

SUNFISH states that with its **key anonymization and data privacy components** (such as the ANM, DS and DM) – **provides technical tools to ensure compliance with the EU GDPR**. SUNFISH integrates its data security components with Data Masking services to support only authorised access to the masking/unmasking services, and masked data. Furthermore, encryption keys and masking tables are stored in SUNFISH blockchain, in order to **ensure such information is kept separately from masked data**. Such information is also encrypted by the Registry Interface and stored in a way that guarantees the security of the storage. Therefore, data processed by DM services are pseudonymised as per the protection scope of the GDPR.

According to the above and the research carried out, the SUNFISH platform seems to contribute to assuring compliance to GDPR, especially with regards to anonymization and pseudonymization techniques as techniques to facilitate data sharing between untrusted parties. However, anonymization is very high maintenance and requires a constant re-evaluation of the risks to re-identification. Therefore, the anonymization component should come with a reservation.

8. [MyHealthMyData \(MHMD\)](#)

MyHealthMyData (MHMD) targets the sharing of sensitive data in an innovative way. MHMD is poised to be the **first open biomedical information network centred on the connection between organisations and individuals**, encouraging hospitals to make anonymised data available for open

research, while at the same time allowing citizens to be the ultimate owners and controllers of their health data. The key elements of MHMD are the following:

- **Blockchain:** a shared public data ledger where information is boiled down into hash language-based codes, which everyone can inspect but no single user controls. This system is used to distribute control of fraudulent activities to the entire network of stakeholders, as any attempt to tamper with whichever part of the blockchain is immediately evident and easily detectable.
- **Dynamic consent:** individuals can provide different types of consent according to distinct potential data uses, also controlling who will access his/her data and for what purpose
- **Personal data accounts:** personal data storage clouds enable individual access from any personal device through the blockchain in a secure, open and decentralised manner.
- **Smart contracts:** Self-executing contractual states, based on the formalisation of contractual relations in digital form, which are stored on the blockchain and automate the execution of peer-to-peer transactions under user-defined conditions.
- **Multilevel de-identification and encryption technologies:** Advanced techniques for encoding and de-associating sensible data from the owners' identity (i.e. multi-party secure computation, homomorphic encryptions), while allowing analytics application to leverage the information.
- **Big data analytics:** applications leveraging the value of large clinical datasets, such as advanced data analytics, medical annotation retrieval engines and patient-specific models for physiological prediction.

The MHMD seems to be a useful tool which supports research initiatives and helps the medical community while at the same time ensuring compliance of hospitals with the GDPR, including the ability for data subjects to exercise their rights, through the dynamic consent, personal data accounts, and at the same time securing their personal data through a combination of advanced security measures such as de-identification and encryption techniques.

Another useful tool is the [MHMD Privacy by design and GDPR compliance assessment](#) to assess and, most importantly, certify the **compliance of the MHMD system to the data privacy and security constraints and requirements set out in the GDPR, a data protection impact assessment (DPIA)** as an **additional deliverable** in the context of WP2- *Regulatory and compliance study*, under the name of **D2.6 – Privacy-by-design and compliance assessment**. The deliverable is freely downloadable [HERE](#). The *MHMD Privacy by design and compliance assessment* describes **MHMD actors** with relevant roles, obligations and responsibilities, **personal data categories and processing operations involved**, **system components** (user and hospital interfaces, data catalogue, blockchain architecture model), **data usage modalities** (i.e., data sharing and secure local computation), **data de-identification measures and system security**.

9. [SHIELD](#)

SHIELD (European Security in Health Data Exchange) aims to unlock the value of health data to European citizens and businesses by overcoming security and regulatory challenges that today prevent this data being exchanged with those who need it.

SHIELD addresses the security and compliance challenges by providing models and analysis tools for **automated identification of end-to-end security risks** and compliance issues which support privacy and 'by design'. In addition, SHIELD defined an open and extensible **data exchange architecture** based on epSOS, able to support security measures to address these security risks. Further, SHIELD developed security mechanisms to deal with **new and emerging risks**, such as inference attacks on sensitive data, and risks from relatively unprotected mobile edge devices. Finally, SHIELD will provide faster and more cost effective methods to **verify and monitor compliance with multiple sets of applicable regulations**. SHIELD also provided guidance in best practices to achieve end-to-end security and data protection compliance in **health and health related applications**. SHIELD will also feed into CEN-Cenelec and ETSI efforts to **create EU standards for data protection by design in eHealth**.

Although the SHIELD integrated solution (SHIELD DevOps) seems to implement security measures according to the risk-based approach, it is not clear from the information provided that the entire solution will ensure compliance with data protection regulations.

10. [gdpr.eu](#)

The [gdpr.eu](#) project provides customizable GDPR Forms and Templates for the most common GDPR forms that companies need in order to be compliant. For example, the [Data Processing Agreement](#) is an important requirement when a data controller engages [Right to Erasure Request Form](#), [Privacy Policy](#). These resources have been deemed as valuable for the purpose of an organisation's compliance and hence will be included in the GDPR Temperature tool.

On the other hand, the [GDPR checklist](#) for data controllers is a very basic tool for the main obligations, providing less information than our GDPR Temperature tool. However, this is a project where we can leverage and show-case their templates and other Guides (such as Data protection and working remotely, Cookies, the GDPR, and the ePrivacy Directive, Everything you need to know about GDPR compliance - [GDPR guides for SMEs](#)).

11. [BPR4GDPR](#)

The BPR4GDPR (Business Process Re-engineering and functional toolkit for GDPR compliance) project provides a holistic framework able to support end-to-end GDPR-compliant intra- and interorganisational ICT-enabled processes at various scales. On the one hand providing a generic framework while fulfilling operational requirements covering diverse application domains.

BPR4GDPR facilitates the enforcement of appropriate organisational and technical measures required for data protection, by automating several aspects of “compliance engineering”. To this end, it will be based on a number of enabling pillars:

- Comprehensive security and data protection policies,
- Incorporation of policies into process models,
- Automatic process models re-engineering in terms of compliance-aware verification and transformation,
- Tools for facilitating run-time compliance enforcement,
- Process mining for the identification of compliance discrepancies and discovery of organisational procedures.

BPR4GDPR has developed a consent management and user-centered tool is a user-centered tool to help organizations increase their compliance with the GDPR by reducing their effort to implement functionalities that are important in the communication to data subjects, such as consent management, right to erasure, right of access, right to rectification, and right to portability. These tools can provide the software architecture to organisations, enabling them to easily integrate them in multiple application fields across boundaries of organisations. The GDPR requirement addressed by this tool is articles 5, 6, and 9, arts. 12-22 (data subject rights) and arts. 25-32 GDPR (articles on security measures). This tool seems to be a good starting point for organisations to automate burdensome obligations such as consent management and recording, and the exercise of data subject rights.

Further, the data anonymization tool tackles recital 26 GDPR which states that the principle of data protection should not apply to anonymous information in a way that the data subject is not or no longer identifiable. The tool anonymizes data in order to guarantee a certain level (quantified) of anonymity through the use of differential privacy. As mentioned by BPR4GDPR itself, this tool can only provide quantifiable anonymity, which is not fully compliant with the WP29 Guidelines on Anonymisation techniques. Anonymisation should be carried out on a case-by-case basis, which calls for qualitative anonymization. Nevertheless, a tool to anonymise can be a great first step to pseudonymization, which can then be further enhanced by a human check and intervention.

Finally, the BPR4GDPR developed a [risk assessment tool](#) which allows users to comply with the need to test the cybersecurity level of the system and the relevant data processing operations. This tool aims to contribute to both article 25 and article 35 GDPR in order to assess the risks and implement technical and organisational measures by design. This tool can also help to raise attention to any high-risk activities that require a Data Protection Impact Assessment.

12. Privacy & Us

The PRIVACY.US **innovative training network** trained thirteen creative, entrepreneurial and innovative early stage researchers (ESRs) to be able to reason, design and develop innovative solutions to questions related to the protection of citizens' privacy, considering the multidisciplinary and intersectoral aspects of the issue. ESRs will be trained to face both current and future challenges in the area of privacy and usability. PRIVACY.US offered a combination of research-related and transferable competence skills that will enhance the career perspectives of the ESRs.

Through this collaborative effort, the project will make a significant contribution and impact to the ESRs future careers. It will also contribute to shaping future privacy policies and practices in Europe and will significantly advance the state of the art in privacy and usability research. However, there are no results that can concretely be leveraged through this project.

13. SPECIAL

The specification and technology proposed by SPECIAL (Scalable Policy-aware linked data architecture for privacy, transparency and compliance) allows for the **acquisition of user consent at collection time and the recording of both data and metadata** and make this information available at all stages of processing. Specifying purposes in the database and establishing an underlying communication link allows data controllers to handle personal data in accordance with the legal provisions and to demonstrate transparency by offering all relevant choices to their customers.

SPECIAL developed technology that supports the acquisition of user consent at collection time and the recording of both data and metadata (consent policies, event data, context) according to legislative and user-specified policies. This is in accordance with the principle of accountability of the GDPR, whereby the controller must provide evidence and demonstrate their compliance. The code is available at: <https://cyberwatching.eu/projects/989/special/products/code-repository>. The tool developed by SPECIAL can provide a manner with which compliance can be demonstrated. In addition, SPECIAL provides a dashboard with feedback and control features that make privacy in Big Data comprehensible and manageable for data subjects, controllers, and processors.

14. CONCORDIA

A project that pilots Cybersecurity Competence Network for Research and Innovation (CONCORDIA) with leading research, technology, industrial and public competences. CONCORDIA provides excellence and leadership in technology, processes and services to establish a user-centric EU-integrated cyber security

ecosystem for digital sovereignty in Europe. It enhances **threat intelligence platform for financial sector** and provides mechanisms for the **access and use control of the data exchanged between different entities**. Concordia will deliver platforms for handling threat intelligence related information and exchanging information for mitigating DDoS attacks. Although it is a project with high potential value in the sector of cybersecurity, it does not seem to tackle any GDPR requirements directly.

15. [CS-AWARE](#)

A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis (CS-AWARE) provides a **cybersecurity situational awareness solution for small- to medium-sized IT infrastructures**. This solution enables detect, classify and visualise cybersecurity incidents in real-time, supporting the prevention or mitigation of cyber-attacks. The solution aims to automate cyber incident detection, classification and visualization through big data analysis tools and methodologies. The CS-AWARE solution aims to provide soft systems-based analysis (SSA) in order to build the organizational cyber security knowledge and identify the monitoring and analysis requirements for cyber situational awareness. The solution of CS-AWARE was created for [Local Public Administrations](#), whether small, medium or large sized. The advantage of this software is that it **can be tailored to any local software set-up, any European language and any type** of LPA internal workflow and specifics. Nevertheless, it is important to note that not enough information is provided in order to conclude that this solution is compliant with the GDPR.

16. [ENSURESEC](#)

End-to-end Security of the Digital Single Market's E-commerce and Delivery Service Ecosystem (ENSURESEC) combines different open-source cybersecurity tools for **protecting the e-commerce ecosystem**. It focuses on cyber-physical threats in the e-commerce ecosystem, from online retailers, though payment services, transport, and delivery stakeholders. ENSURESEC involves six main modules:

1. **Prevention by design:** Prevention assesses and certifies that the design of the system interfaces is secure against certain classes of critical attacks and vulnerabilities.
2. **Detection by monitoring:** Detection monitors run-time interface operations at the application level and network level for resilience against both known and unknown threats.
3. **Response and mitigation of threats and incidents:** Whenever a vulnerability or arbitrary malicious activity is detected, the system continues operation in fail-safe mode while the response and mitigation engine communicates an appropriate response to the affected users and partners and attempts to mitigate the impact.
4. **Recovery of compromised interfaces:** The recovery engine recovers the system's state by identifying what has gone wrong based on a dependency-directed diagnosis.
5. **Resilient-oriented situational awareness:** ENSURESEC develops live security monitors based on the resilient-oriented situational awareness component that employs advanced machine learning techniques to continuously detect any suspicious and evitable incident and visualize its impact and interdependencies at a different level.
6. **Training of SMEs and their citizen clients:** To handle inevitable threats and promote trust and resilience, ENSURESEC conducts interactive and serious games-based training and awareness to make citizen clients of e-commerce business partners (SMEs) aware of potential security threats and train on how to avoid them.

The ENSURESEC solution can be relied on to support organisations' activities for compliance on the area of personal data breaches, especially breaches of data confidentiality or breaches related to staff and customers. This tool can be helpful for stakeholders that have e-commerce websites in order to ensure that their activities are protected by design and that the personal data obtained are treated according to the standards posed by the GDPR.

17. [SANA](#)

Service Analysis, Notification and Alerts (SANA) is a security alert system, which allows organisations to be aware of any incidents related to your systems or integrated into your applications. SANA is part of Hispasec, an SME, as one of the longest-lived and best-appreciated services by customers. SANA scans for vulnerabilities, provides a complete dashboard of alerts on vulnerabilities, updates and patches of software in terms of computer security, allowing to know at all times any vulnerabilities that may affect the products of the company or company use daily. The SANA service can be a useful tool to ensure that the majority of security incident will be alerted in the company. However, this service does not directly seem to recognize the personal data breaches defined by the GDPR. Therefore, although this may be a useful tool for the general overview of security incidents, it does not directly raise awareness of the incidents that have personal data implications.

18. [CyberWISER](#)

Wide-Impact Cyber Security Risk Framework (WISER) is a novel model-based cyber-risk management framework able to assess and mitigate cyber risks in real time, also incorporating socio-economic impacts of cyber risks. The WISER Framework is a risk platform as a service (RPaaS) consisting of three modes of operation that collectively represent the WISER [portfolio](#):

1. CyberWISER Light, targeting **SMEs** and providing a user-friendly tool to increase awareness through self-assessment.
2. CyberWISER Essential targeting **SMEs** and ICT systems in general, and providing a pre-packaged solution for real-time risk assessment.

3. CyberWISER Plus targeting highly **complex cyber systems** such as **critical infrastructures**, and providing on-demand services for real-time and cross-system assessment of cyber risks.

In addition, WISER facilitates the uptake of a cyber-security culture through a series of free services:

1. CyberWISER SEIT, an online tool that calculates the estimation of economic and non-economic impacts of cyber attacks on an organisation. Impacts can be direct or indirect. Target audiences: **SMEs** and **small IT teams** in public administration.
2. Cartography of European Cyber Security Strategies: an interactive map that analyses national cyber security strategies in terms of capacity building, legal frameworks, public private partnerships and best practices for risk management with downloadable reports.

CyberWISER provides affordable cyber risk assessment services to SMEs. It is also useful that WISER uses both an online-centered delivery model and a customised approach (through a team of experts “on-call”, where applicable), to overcome the intrinsic shortfalls of the one-fits-all solution. Therefore, this layered solution can be of help to SMEs in their general cybersecurity posture, however, it does not seem to address any of the legal, data protection requirements introduced by the GDPR.

19. [CANVAS](#)

CANVAS provides an integrative view on the ethical and regulatory issues of cybersecurity, by unifying technology developers with legal and ethical scholar and social scientists to approach the challenge how cybersecurity can be aligned with European values and fundamental rights. CANVAS has **identified several gaps with respect to ethical research and European cybersecurity regulation that need to be addressed**. In 14 workshops, CANVAS has unified several dozen experts of cybersecurity with a particular focus on non-technical aspects. This expert pool **provides a resource for future projects that want to focus on responsible research and innovation in cybersecurity**. Through its **teaching material**, CANVAS provides the foundation that the future generation of cybersecurity experts obtains basic insights and knowledge on how to tackle ethical and legal dilemmas in cybersecurity. All CANVAS results are freely available on their website, including:

1. The [CANVAS Briefing Packages](#); a set of summarized, easily digestible information on challenges as well as possible, value-driven solution approaches linked to European cybersecurity policy.
2. The [CANVAS Reference Curriculum](#) on value-driven Cybersecurity; a whole package of material (lecture slides, case studies, videos, text resources) with the goal to integrate the value perspective into cybersecurity design decisions, with a focus on academia and industry training programs.
3. The [CANVAS massive open online course](#) (MOOC) that transports the main insights of CANVAS to a broad public and that provides a comprehensive overview of the central principles and challenges in the fields of cyber security, privacy and trust.
4. The [CANVAS book "The Ethics of Cybersecurity"](#) that discusses the full plethora of ethical aspects of cybersecurity and has a strong practical focus, including case studies that outline ethical dilemmas in cybersecurity and guidelines and other measures to tackle those dilemmas.

Although this is not a resource that directly satisfies the main requirements recognized by the GDPR, it has created a useful set of resources that could complement the obligations of the GDPR. For example, the principle of data protection by design has its core as data protection however fairness by design is a requirement that goes hand in hand too. Therefore, CANVAS' results may not directly address the requirements of the GDPR, and will thus not be embedded in the GDPR Temperature Tool. However, the results of CANVAS can further enhance the GDPR requirements and compliance posture of an organization, and can be relied on by stakeholders developing cybersecurity solutions with ethical implications.

20. [E-SIDES](#)

Ethical and societal implications of Data Science (E-SIDES) aim to complement the research on privacy-preserving big data technologies, by **identifying, mapping and analysing the main societal and ethical challenges** emerging from the **adoption of big data technologies**, conforming to the principles of responsible research and innovation; setting up and organizing a sustainable dialogue between industry, research and social actors, as well as networking with the main Research and Innovation Actions and Large Scale Pilots and other framework programme projects interested in these issues. E-SIDES has successfully delivered 16 workshops, and produced many deliverables and outputs such as a [Common Glossary of the key terminology](#), [Refined Research Framework](#), [Lists of ethical, legal, societal and economic issues of big data technologies](#) (identifying and analysing the most relevant ethical, legal, societal and economic issues implicated by the development of big data technologies). In its [Overview of Existing Technologies](#) E-SIDES provided insights into the existing approaches, methods and technologies that may have the potential to address ethical, legal, societal and economic issues raised by big data applications. Among the issues identified are threats to privacy and self-determination, strong interdependencies, limited trustworthiness and lack of accountability. In addition E-SIDES provided an assessment of privacy-preserving technologies [Assessment of Existing Technologies Under Development](#) by assessing the extent to which ethical, legal, societal and economic design requirements

are relevant and creating an inventory of the impact assessment modes and tools of data-driven innovation and privacy-preserving technologies. Another interesting deliverable was the [Overview of design requirements](#), describing design challenges faced in the context of privacy-preserving technologies paying particular attention to the requirements faced in the context of big data. White papers from the key deliverables for dissemination.

- [Real-Life Examples of Big Data Implications](#)
- [Which data technologies play a key role to preserve privacy and security?](#)
- [How effective are privacy-preserving technologies in addressing ethical and societal issues?](#)
- [Privacy-preserving technologies are not widely integrated into big data solutions. What are the reasons for this implementation gap?](#)
- [Implications of the General Data Protection Regulation - A Media Analysis](#)

Although E-SIDES does not provide a tool for compliance - in the stricter sense – it does provide a range of useful documents, research results and methods that can be used for the designing, development and research of privacy enhancing techniques.

21. TYPES

Towards transparency and privacy in the online advertising business (TYPES) planned to demonstrate solutions that protect individuals' privacy while empowering the users to control how their data is used by service providers **for advertising purposes**. TYPES makes it easier to verify **whether users' online rights are respected** and if personal data is **exchanged** for a reasonable value-added to users. The project aims to tackle the **lack of transparency** regarding tracking techniques and the type of information companies collect about users. Software tools for implementing total mitigation (e.g., ad blocker or cookies blocker) have been released to block any transfer of information from end users towards the online advertising ecosystem.

TYPES has created 3 different tools which should enable the end user to **configure the privacy settings** so that only the information allowed by the end-user is collected by online advertising platforms, to **understand the flow of their information** within the online advertising ecosystem and how it is being used, to **detect episodes of information collection** occurring without consent and identify the offender; and to **know the value of their data**

The 3 different tools are the following

1. [Data Valuation Portal](#)

The [Data Valuation Portal](#) informs users how advertisers target users, the kinds of personal information available on the ad-market, and the financial value of it. For this purpose, the back-end crawlers collect bidding data from four major advertising platforms using a combination of targeting options provided by the platforms. Interested users can select one of the advertising platforms and choose a combination of demographic and behavioural data that describe a given online user, then the portal displays the monetary value of that profile and its evolution over time. This portal is targeting the users' side, rather than the organisations' side. However, this tool can be re-directed by organisations that want to increase transparency and awareness of how targeted advertising takes place. Nevertheless, due to the scope of this tool it will not be embedded in the GDPR Temperature tool.

2. [eyeWnder](#) (Real Time Web Advertisement Analyser)

eyeWnder is an experimental browser add-on for detecting Online Behavioural Advertising and shedding light to some of its underlying workings. The software relies on the participation of users like you to achieve its goal which is to increase transparency in online advertising. This tool can no longer be accessed and the link to it is unsafe.

3. [FDVT](#)

Finally, the Data Valuation Tool for Facebook™ Users (FDVT) tool aims to inform in real-time Internet end users regarding the economic value that the personal information associated to their browsing activity has generated. Due to the complexity of the problem, the tool's scope is narrowed down to Facebook™ i.e., inform Facebook™ users in real time of the value that they are generating to Facebook™. This tool is an easily [downloadable from Chrome or Firefox](#). As with the Data Valuation Portal, this tool has been created facing the users rather than the organisations. This is the reason why this tool, although it raises awareness of the ad-tech industry, targeted advertising, and profiling, it has been chosen to stay out of the GDPR temperature tool due to its scope. However, the FDVT is a transparency tool that organisations can nevertheless promote in order to enhance the transparency of the advertising industry.

22. SOFIE

The goal of Secure Open Federation for Internet Everywhere (SOFIE) is to enable diversified applications from various sectors to utilize heterogeneous IoT platforms and autonomous devices across technological, organizational and administrative borders. This should be done in an open and secure manner, making reuse of existing infrastructure and data easy. SOFIE aimed to create business platforms, based on existing IoT platforms and distributed ledgers, without needing to negotiate with any gatekeeper (neither technology- nor business wise).

The product created by SOFIE is the [SOFIE Privacy and Data Sovereignty](#) (PDS) component, which provides mechanisms that allow actors to better control their data, as well as mechanisms that protect client privacy.

PDS enables the creation of privacy preserving surveys. These are surveys that allow users to add noise to their responses using local differential privacy mechanisms. The addition of the noise prevents third parties from learning meaningful information about specific users, but at the same time meaningful aggregated statistics can be extracted. PDS also implements an OAuth 2.0 Authorisation Server. This server accepts authorisation grants and, if the grant is valid, it generates an access token encoded using the JWT format. Accepted types of authorization grants are: Decentralised Identifiers (DIDs), Verifiable Credentials (VCs), and pre-shared secret keys. The generated access token can be used by any Web service, as well as with SOFIE's IAA component. SOFIE's PDS component can be embedded in different organisations that wish to increase the security of their IoT devices and infrastructure. However, it cannot be guaranteed that this security measure is appropriate for all levels of risk identified. This means that the PDS is not a single solution relevant for all risk levels, and may need to be complemented by other security measures or tools as well. In addition, the PDS does not seem to have considered the level of risks to which the implementation of the PDS is appropriate. For this reason, the PDS component has not been embedded in the GDPR Temperature Tool.

23. [FENTEC](#)

The project Increasing trustworthiness of ICT solutions by developing Functional ENcryption TEChnologies (FENTEC) aims to make the functional encryption paradigm ready for a variety of applications, integrating it in ICT technologies as naturally as classical encryption. The primary objective is the efficient and application-oriented development of functional encryption systems. FENTEC's team of cryptographers, software and hardware experts and information technology industry partners will document functional encryption needs of specific applications and subsequently design, develop, implement, and demonstrate the applied use of functional cryptography. The project's mission is to develop new Functional Encryption (FE) as an efficient alternative to the all-or-nothing approach of traditional encryption. The tool of [Privacy-Preserving Statistical Analysis](#) is to enable clients to perform analytics with their clients' data guaranteeing the privacy of it through the implementation of cryptographic API of Functional Encryption system. This tool is useful for organisations who want to carry out analytics on the data of their clients, without compromising the data protection aspects. Overall, the GDPR mentions encryption as one of the manners with which personal data can be safeguarded (recital 83, Article 32 (1(a)), etc.), as well as the considerations that can lower the severity of a data breach, if it takes place. Therefore, this tool surely has potential to increase the compliance of an organisation.

24. [WITDOM](#)

The project of empOWering prIvacy and securiTy in non-trusteD enviroNments (WITDOM) has **delivered automatic and efficient privacy provisioning solutions**, which cover varying needs of **privacy for data** that must be handled by **non-trusted third parties**, ensure higher flexibility by **dynamic adaptation to user needs and privacy preferences**. In summary, **privacy is preserved by keeping data confidential (encrypted and privacy-protected) in the un-trusted environment**, while the data owner can operate with and make use of the data in the encrypted domain. Specifically, [WITDOM Data Masking](#) component is responsible for **masking sensitive data classified as direct identifiers**. The masking process creates service-and-user-specific tokens that can be updated over time, satisfying two main security requirements: irreversibility and unlinkability.

[WITDOM's data masking](#) component can be utilised as a security measures for sharing data or for storing data in non-trusted environments. Based on the description given by the WITDOM project, it classifies sensitive data as a direct identifier and instead masks it through a process that creates service-and-user specific tokens that can be updated over time. The Article 29 Working Party has identified three different criteria in order to ensure anonymisation, linkability, singling out and inference. This product satisfies the first requirement, as well as the requirement of irreversibility. As a result, the two requirements of singling out and inference are not fulfilled and therefore this product does not offer anonymisation. Nevertheless, pseudonymisation or masking can be an appropriate security measure to implement – especially if the personal data is in an untrusted environment. Therefore, we would recommend WITDOM's data masking component as a security measure.

25. [SUPERCLOUD](#)

The User-Centric Management Of Security And Dependability In Clouds Of Clouds (SUPERCLOUD) proposed new security and dependability infrastructure management paradigms that are on the one hand user-centric and self-managed. It is user-centric because it is a self-service clouds-of-clouds where customers define their own protection requirements and avoid lock-ins; and self-managed for self-protecting clouds-of-clouds that reduce administration complexity through automation. The tool which was

developed by SUPERCLOUD is the [Data Anonymisation Tool](#). Data anonymization techniques open the possibility of **releasing personal and sensitive data**, while **preserving individual's privacy**. The data anonymization tool in this context is among others based **on k-anonymity**, whereby the focus is put on the **irreversibility of the released data**. The tool aims to calculate the best solution for the given data in terms of cost-efficiency. This is done by means of so-called cost metric calculation as well as the Optimal Lattice Anonymization (OLA) algorithm. A detailed explanation of the OLA algorithm as well as of all including components of the tool can be found in the Deliverable D3.2 of SUPERCLOUD released in the second project period.

Based on description it is compliant with the Article 29 WP and the Spanish Data Protection Authority's guidelines on k-anonymity. However, we cannot access the tool due to errors and lack of domain of the project. Therefore, this will not be embedded into the GDPR Temperature tool and cannot guarantee compliance with the GDPR.

26. [OPERANDO](#)

Online Privacy Enforcement, Rights Assurance and Optimization (OPERANDO)'s goal is to specify, implement, field-test, validate and exploit an **innovative privacy enforcement platform** that will enable the **Privacy as a Service (PaS) business paradigm** and the market for online privacy services. The OPERANDO project integrated and extended the state of the art to create a platform that will **used by independent Privacy Service Providers (PSPs)** to provide comprehensive user privacy enforcement in the form of a dedicated online service, called "Privacy Authority". The OPERANDO consortium aims to contribute to the entire ecosystem of online privacy stakeholders: Users, PSPs, Online Service Providers and Regulators. To increase transparency of the privacy services and dissemination of results, **OPERANDO outcomes will be implemented in Open Source**, and will be made available to the community for evolution and value-adding beyond the scope of the project.

The tool [PLUSPRIVACY](#) provides users with a **unified dashboard for protecting yourself from a variety of threats to your privacy**. It enables data subjects to **control the privacy settings in their social network accounts, hide their email identity, block ads**, trackers and malware and **prevent unwanted apps** and browser extensions from **tracking you** and collecting your private data.

There are four main functions for your benefit:

1. Privacy for benefit deals - When you use social media sites valuable data is collected about you by these sites. The economic value of this data is blocked to you, the user. PlusPrivacy allows you to benefit from this data sharing if you wish.
2. Identities - PlusPrivacy allows you to set up email aliases and substitute identities which can be instantly wiped out. The credentials of these accounts are managed for you automatically.
3. AdBlocking and anti-tracking - Social networks allow other sites or Ad networks to track you when you visit them. User privacy is violated and your identity is disclosed without you realizing this. PlusPrivacy enables you to filter out third party tracking and ads allowing you to control the level of tracking or sharing.
4. Dashboard - PlusPrivacy offers a unified privacy settings dashboard where you can handle all your accounts in one place.

Giving control back to the users is not a simple task. The [PlusPrivacy dashboard](#) can be used by service providers in order to offer privacy services to their data subjects. PlusPrivacy will give individuals the ability of changing their privacy settings according to their wishes. PLUSPRIVACY provides a unified dashboard for controlling the settings of social network accounts, hiding the e-mail identity, blocking ads, trackers and malware as well as preventing unwanted apps and browser extensions from collecting private information and tracking them. Although GDPR compliance cannot be guaranteed simply by embedding

27. [AXENCE](#)

Axence is a Polish SME that provides professional solutions for the comprehensive management of IT infrastructure for companies and institutions all over the world for more than 13 years. Axence software has more than 700,000 installations in 175 countries.

The product [nVision10](#) Axence nVision® is a paid product which responds to the key needs of IT administrators and security officers in the scope of network and user monitoring, hardware and software inventory, remote technical support and data protection against leakage. It **enables the management to optimize the operating costs of any IT infrastructure, regardless of its size**.

28. [GuardYoo](#)

GuardYoo is an online Platform delivering fully automated Compromise Assessment audits with Forensic Analysis. GuardYoo uses context to **identify any anomalies that occur within a network**, which means it identifies if something has slipped past existing security solutions and is hiding without the knowledge of the client. Historically an audit this type of audit, would involve deploying a team of consultants on-site for 6-8 weeks to collate data, with a further 4 weeks to compile the report. GuardYoo engine analyses

existing Log Data to deliver a **Compromise Assessment within 1 week**. GuardYoo makes Compromise Assessment affordable to SME companies by automating the process. GuardYoo will deliver a variety of services such as full asset discovery, suspicious user behaviour, suspicious admin account behaviour, poor cyber policies, identification of unauthorised software and full password strength analysis.

GuardYoo is an automated compromise assessment platform developed by an SME. Based on the information provided, it is a solution for forensics analysis of the network, and it seems to deliver an audit relatively shortly, within 1 week, in comparison to how long it would take for a consulting team to carry it out (4-8 weeks), it is still not considered GDPR compliant. In order to ensure that a personal data breach is detected as soon as possible it would need to immediately alert of such event. However, this may be unrealistic a therefore, this tool can act as a preventative – bird-eye vision of the network. However, there would need to be another system in place in order to ensure that the personal data breach is detected as soon as possible and communicated to the supervisory authority or the data subjects (should there be a high risk to the data subject) within 72 hours.

29. [Fitsec Ltd](#)

Fitsec Ltd is a Finnish cyber security company founded in 2009 and is an SME. We offer cyber security services with a strong focus on preventing and detecting targeted attacks. Over the years, we have developed innovative cyber security products to complement our services, always focusing on our customers actual needs. Fitsec Ltd provides an [Asset tracker](#) which can be found in Cyberwatching.eu's Marketplace. The Asset tracker assists organisations in detecting their data leaks. Specifically, this service enables them to track personal data of an organisation and check if the data has leaked to the internet. Tracking this information for an organisation that handle personal data enables the organisation not only to have a quick response to the Supervisory Authority (within 72 hours of the personal data breach) but it also helps minimize the risks to the data subjects. In addition, the SME can help isolate and fix weaknesses in the organisation's security in order to ensure that the security gap has been adequately filled. The service also helps organizations to fulfil the requirement of notifying affected parties in the event of a data breach, as outlined in the GDPR.

Assets, or information related to the organization can be for example: email addresses, IP addresses, domain names or payment card information.

The service is easy to use and does not require any installations in your environment. From the easy-to-use [web interface](#), you can see the assets being monitored, add new assets to be monitored and analyze any matches that have been found. All findings are reported to you in whatever way you desire.

30. [CLYM](#)

Clym is the **data privacy platform** that helps organisations **meet their data protection obligations**. Cookies, Consent, Requests, Policies and more are all managed in a secure and adaptive application.

Clym helps you **collect, control and manage the data that is relevant for your company** in a transparent way. [Clym](#) is a platform provided by an SME in the United Kingdom and it aims at **website compliance**. It covers 6 main areas of compliance, namely: **Data consent management, Cookie consent management, Company & DPO data management, Terms, Policies, Agreements & Procedures, Data subjects' requests, Localisation and Consent receipts**. This platform can assist data controllers to comply with the GDPR by having a full picture of the data subjects' wishes by creating a timestamped, audit-ready and scalable workflow to accommodate consumer access requests. In addition, the platform aids organisations in managing their data protection policies and procedures by: timestamping each modification, managing each policy centrally, and demonstrating the organisation's evolution in transparency through a version control functionality. This platform helps increase transparency, respect the data subjects' rights and allow them to exercise them in an organised and easy manner, and ensure that cookies are implemented in an appropriate and transparent manner. Finally, the Clym platform can be easily integrated into all major platforms for web design and development.

ANNEX F. GLOSSARY

Term	Explanation
AI	Artificial intelligence
DEP	Digital Europe Programme
DPIA	Data Protection Impact Assessment
DSP	Digital Service Providers
EDPB	European Data Protection Board
EPBS	European Data Protection Supervisor
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
IoT	Internet of Things
NIS	The Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union <i>OJ L 194, 19.7.2016</i>
OES	Operators of Essential Services
R&I	Research and Innovation Projects, consisting of the European Projects
SAs	Supervisory Authorities
SMEs	Small and Medium Enterprises
WP29	Former Article 29 Working Party, now the European Data Protection Board