cyberwatching.eu

The European watch on cybersecurity & privacy

Covid-19 Pandemic – A New Crisis In Privacy

Insights and recommendations from Cyberwatching.eu

2021

cyberwatching.eu consortium

Trust-IT Services
Communicating ICT to markets

Oxford e-Research Centre

University of Oxford

ICT Legal Consulting
Balboni Bolognini & Partners

European Digital SME Alliance

CONCEPTIVITY

360 SECURITY

AON

aeiciberseguridad
Agrupación Empresarial Innovadora CIBERSEGURIDAD y Tecnologías Avanzadas

Table of content

Table of figures

Disclaimer

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 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.

1 Introduction

"MAKING EUROPE SAFER. A new cybersecurity strategy to build trust and resilience".

*Video Talk held on 27 January 2021 with **Lorena Boix Alonso**, Director 'Digital Society, Trust and Cybersecurity', DG CNECT, European Commission*

The COVID-19 pandemic has created a **hitherto unforeseen environment where the dependency on digital information, data privacy and IT security were of paramount importance**. Whilst physical human contact has reduced, the usage of digital communications and exchange of data has exploded at an unprecedented rate. People were forced to work from home without much prior notice. Business and organization data has been migrated from IT secure systems to personal devices. Families have relied on digital means of communication to maintain social ties. The elderly have found themselves needing to adapt to such means of communication to keep in contact with loved ones. Governments have struggled between controlling the pandemic, enforcing measures to protect citizens but faced with the issues surrounding data privacy. **The combination of these requirements and behaviours has led to paradigm shifts that raised weakness and threats which thus far did not exist.** With sudden limits on personal movement, workplace shifts, health reporting, health tracking, data privacy has become an even more sensitive and important topic to address.

2 Survey on Privacy Risks Related to Covid-19

In July 2020, in the early stages of the pandemic, Cyberwatching.eu partners generated an online survey in the context of Covid-19 on Cybersecurity and Privacy, to understand the change in social interactions and at the same time understand the society's opinions on the risks of sacrificing some of their privacy for the public interest, [1] which also focused on the Covid-19 contact tracing apps.

Through this survey, Cyberwatching.eu was also able to collect information relating to society's acceptance of the sacrificing of their privacy, and whether they deemed it as a justified approach. The fact that cybersecurity services in the healthcare sector are directed towards citizens cannot be ignored, thus the response of individuals will be used as an indicator of the risks of cybersecurity services from the perspective of citizens. **In COVID-19, citizens realised that our ability to exist relies on electronic communications and it has been insightful to analyse the responses**.

2.1 Dissemination of the Survey

The survey was widely distributed as follows:

- AEI sent the survey to 210 email addresses from 196 different Cyber and ICT clusters
- AEI sent to their 70 members
- AEI through Twitter (+3100 followers)
- Digital SME through their social network
- CONCEPTIVITY to ECSO partners to + 230 companies via their newsletter
- CONCEPTIVITY through LinkedIn, + 7000 contacts
- CONCEPTIVITY to EOS - published in the EOS newsletter
- CONCEPTIVITY through personalized messages

[1] The survey can be found at the following link: https://cyberwatching.eu/online-survey-cybersecurity-and-privacy-Covid-19 or in Annex 1.

- Cyberwatching.eu web site's portal contained the survey for 8 months
- ICTLC through their social network channels (Twitter, and LinkedIn)
- ICTLC through their newsletter and news blog
- TRUST-IT to the Concertation list (+ 43 contacts)
- TRUST-IT to the contacts from the H2020 projects database, some + 150 project contacts

2.2 Response to Survey

A total of **83 citizens responded to the survey**. As seen in Figure 1, the survey responses covered not only many European Member States, but also international responses from countries like Japan, the United States of America and Saudi Arabia. This can be interpreted as a positive attitude and interest of stakeholders, both in Europe and internationally, to understand how societal perceptions have changed as a result of Covid-19.

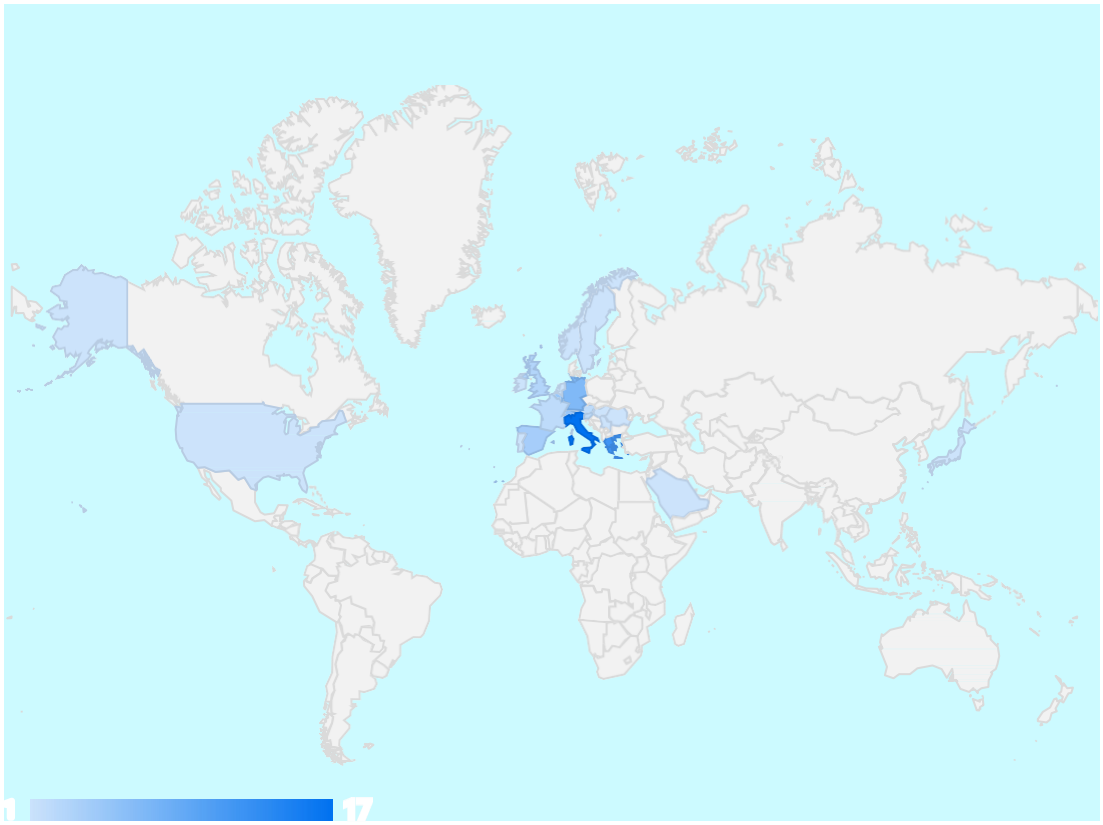

Figure 1: Response to survey by the country

3 Challenges of Covid, Contact Tracing Apps and Privacy

Largely, the positive and wide response was also reflected in the results of the survey. It was easy to observe openness and flexibility towards the idea that, during Covid-19, privacy is relative. The following section addresses the findings from the survey, with conclusions or recommendations, as applicable.

3.1 European Landscape on Contact Tracing Apps and Privacy

According to the European Commission, **twenty-one out of the twenty-seven European Member States has deployed a contact tracing app in their country**[2]. According to the latest publicly available information, two more countries are currently developing a contact tracing app, while four countries are not foreseeing the deployment of a contact tracing app.

These facts emphasise that contact tracing apps have become the norm, considering that the pandemic continues to evolve in the European continent. Therefore, **this document supports the European cybersecurity services to understand what the risks are in the current situation, and what recommendations can arise to improve**. The Cyberwatching.eu consortium approached these risks by trying to understand the citizens' perspective towards contact tracing apps to identify the risks that remain unclear or important from the perspective of society.

Based on research, there are several protocols that can be found in the current digital contact tracing app market.[3] Although many kinds of contact tracing apps exist this research illustrates three different protocols.

- **Protocol 1** consists of the app recording its own location, and once a user is reported as being infected, their trajectory is sent to the authority.[4] The authority in hand would then share the pseudonymous trajectories of all infected users with every user, which would require each user to check whether they were in close contact with an infected individual.
- **The second protocol** relies on the broadcasting of a unique identifier through Bluetooth, so that when two phones are in close proximity, they can exchange identifiers. If a user is infected, the authority would contact all users that came in close proximity through their unique identifier.
- **The third protocol** considers similar broadcasting of a unique identifier via Bluetooth which is reset every hour. In this case, if two phones came in close proximity, they would exchange identifiers; and if one user was infected, all identifiers that they have used would be sent to the authority. The authority would then share the identifiers of all infected users with every user, and users would check if they encountered one of these identifiers. This research was used as an example in order to question the extent to which data protection can be guaranteed during the development and deployment of such apps. It is an interesting approach that could be further enhanced in order to help app developers and stakeholders create contact tracing apps according to data protection by design and by default. In addition,

[2] Specifically, that includes Austria, Belgium, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Malta, Netherlands, Poland, Portugal, Slovenia, Spain. More details could be found here: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en.

[3] Yvyes-Alexandre de Montojoye, Florimond Houssiau, Andrea Gadotti, Florent Guepin, *Evaluating Covid-19 contact tracing apps? Here are 8 privacy questions we think you should ask,* available at: https://cpg.doc.ic.ac.uk/blog/pdf/evaluating-contact-tracing-apps-here-are-8-privacy-questions-we-think-you-should-ask.pdf.

[4] Yvyes-Alexandre de Montojoye, Florimond Houssiau, Andrea Gadotti, Florent Guepin, *Evaluating Covid-19 contact tracing apps? Here are 8 privacy questions we think you should ask,* available at: https://cpg.doc.ic.ac.uk/blog/pdf/evaluating-contact-tracing-apps-here-are-8-privacy-questions-we-think-you-should-ask.pdf, p.2.

the EDPB has published useful guidelines for contact tracing applications, which can be used as a baseline for the development of cybersecurity services in this context. [5]

According to independent research on contact tracing apps[6] requested by the Dutch Ministry of Health, one of the main conclusions was that all of the contact tracing apps available in the Dutch market struggle to comply with the GDPR.[7] The Dutch Ministry of Health required solutions to meet the principles including anonymity (untraceable to individuals) of the data processed, accuracy (minimising false positives), data minimisation, disclosure (strict data sharing policy), purpose limitation (the process of source and contact tracing is the sole purpose of processing), transparency (including the ability for users to report errors and vulnerabilities), security, deletion (when the contact tracing app is no longer needed, the data should be deleted), and lawfulness (GDPR compliance).

The **results of the research** both identified gaps for contact tracing apps, but also confirmed their (potential) compliance with several principles. On one hand, the **principle of anonymity could not be guaranteed** by any of the apps, and the **principle of accuracy seemed to be dependent on the strength of Bluetooth connections as well as on whether the user and their device were in the same location**. On the other hand, **data minimisation and purpose limitation were both respected** by storing minimal information of the device and for the envisaged purpose (of contact tracing). The disclosure of the data had a tendency to be based on the user's consent, and the legal basis of apps processing pseudonymised data was Article 9 (2) of the GDPR and Dutch requirements of the Public Health Act. Lastly, all **contact tracing apps had the potential to meet both the transparency principle and the principle of data deletion**.[8]

The above conclusions indicate that although contact tracing apps in the Dutch market have the potential to be compliant with the GDPR, there are certain principles that must be more carefully evaluated and implemented, including the principle of anonymisation, and the principle of accuracy.

In congruency with the results of the Dutch Ministry of Health, **the need for guidance on contact-tracing apps has been recognised on the supranational level**. Several international and EU institutions have published reports, guidance, guidelines, recommendations, best practices, conditions and obligations applicable to contact tracing apps. Nevertheless, since health-related data is a category of personal data that allows for further specifications and limitations on the national level, many Data Protection Authorities have published their own set of conditions and guidance for providers of contact tracing apps to follow.

Data Protection Authorities of Europe have supplemented the European guidance in order to provide the national data protection requirements and best practices when processing personal data in the context of contact tracing and tracking applications. In fact, the Consortium has collated the various guidance on processing of personal data during the Covid-19 pandemic, as well as on the topic of contact-tracing, in the News section of the website – which serves as a knowledge mapping of some of the main official resources,[9] and that includes many published reports not only from Europe but also from countries all over the world.

Nevertheless, it has been observed that the use of contact tracing apps is dependent on the people's perception of their risks and social preferences, rather than on the possible benefits to society and

[5] European Data Protection Board Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak, p. 11.

[6] Specifically, the analysis was carried out on the responses to the Ministry of Health's invitation to the market for proposals for smart digital solutions for contact tracing during the Covid-19 pandemic.

[7] Juridische analyse - advies Autoriteit Persoonsgegeven inzake de DPIA van de CoronaMelde, available in Dutch at: https://www.rijksoverheid.nl/documenten/publicaties/2020/04/19/samenvatting-privacy-analyse-contactonderzoeksapps.

[8] Note that the adherence of the security principle was left to be addressed by an independent report carried out by security experts.

[9] Note that due to the speed and number of updates or new publications on the topic, there is no presumption of completeness of this list.

public health.[10] Several research initiatives have shown that, on the one hand, the widespread adoption, and on the other, the efficiency of the contact tracing apps remains relatively low.[11]

3.2 Findings from the Survey with respect to Contact Tracing

The online survey on Cybersecurity and Privacy also placed focus on the Covid-19 contact tracing apps, and results illustrated that when it comes to contact tracing/tracking applications, which are specifically introduced by the government or a public authority, 62% of the respondents' governments had a governmental tracing or tracking app. The respondents with the highest positive responses came from countries including Italy, Austria, Germany, France, and Switzerland. Nevertheless, only 50% of the citizens that had an available contact tracing app actually used it. It is also worth noting that out of the 21 countries that have a contract tracing app currently, 20 have the potential to become interoperable but only 50% of them are actually interoperable. Interestingly, the majority of the respondents (79%) did not feel that they sacrificed their privacy during Covid-19 although only 21% of the respondents felt they had sacrificed their privacy, another 29% did not use the very app because it could potentially compromise their privacy. This means that even if they did not explicitly feel that their privacy was being sacrificed, a large proportion of the respondents did not actually use the contact tracing app. It is worth noting that out of the respondents that felt they had sacrificed their privacy, 70% of them thought that this sacrifice was not justified. The reasoning of those respondents was that privacy violations lead to violations of their freedom, and abuse of their personal data by enforcement or by the government.

Further, only 12% responded that the tracing app was mandatory to use, or that it was mandatory during the peak of Covid-19. At a first glance, the voluntary nature of the application may be a non-privacy related reason for which the respondents did not use the tracing app. However, when asking participants, the reasoning for not using the tracking app, the response was overwhelming that it **related to privacy and movement tracking concerns**. One participant even compared the contact tracing app with "big brother", which may be a hyperbole, but nonetheless, it emphasised the lack of trust of the participant towards the contact tracing app. The fact that 12% of respondents mentioned that the tracing app was mandatory, also goes against the recommendations given by the EDPB to ensure that the use of contact tracing applications should be voluntary.[12] Specifically, the EDPB notes that voluntary adoption is the only way with which systematic and large-scale monitoring of location and/or contacts, which is a “grave intrusion into their privacy”, can be legitimised. [13]

On the question of whether the respondents’ trust that their government or public authority protected the personal data they shared or would share through the contact tracing app, the results were concerning. Almost half of the respondents, to be precise, **two in five (42%), did not trust that their government would protect their personal data**. As has been mentioned by the EDPB, data protection is “indispensable to build trust”, as well as to create the conditions for social acceptability of solutions such as contact tracing apps. [14] Therefore, the lack of public trust may also be reflected in the eventual success of these apps.[15] In addition, 38% of respondents were concerned that during

[10] Yves-Alexandre de Montjoy, Tarun Ramadorai, Tomasso Valletti, and Ansgar Walther, *A simple Theory of Contact Tracing Applications*, Imperial College London, September 2020, p.8, available at: https://imperialcollegelondon.app.box.com/s/ojm4rryi15mua3p52zpas93heucd2qm0 .

[11] SensorTower, *Covid-19 Contact Tracing Apps Reach 9% Adoption in Most Populous Countries*, July 14, 2020, available at: https://sensortower.com/blog/contact-tracing-app-adoption, and Rodríguez, P., Graña, S., Alvarez-León, E.E. *et al. A population-based controlled experiment assessing the epidemiological impact of digital contact tracing*. Nat Commun **12,** 587 (2021). https://doi.org/10.1038/s41467-020-20817-6.

[12] Paragraph 24 of European Data Protection Board Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak.

[13] Paragraph 24 of European Data Protection Board Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak.

[14] Paragraph 3 of European Data Protection Board Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak.

[15] Achieving Privacy by Design in Contact Tracing Measures - Global Privacy Assembly, available at: https://globalprivacyassembly.org/contact-tracing-statement.

the Covid-19 crisis their personal data would be controlled or monitored by the government. One participant mentioned that when tracking individuals, the linking of data sets should be ensured. For example, administrative data (such as age, or localisation) should be separated from health-related data (such as other underlying diseases).

In conclusion, contact tracing apps may at the moment be widely available in Europe, however, their **adoption remains doubtful (50%)**. In addition, although most did not feel like their privacy was sacrificed through the contact tracing app, those that did felt that it was not justified. This can be further explained by the fact that many respondents did not trust that their government would protect their personal data. Nevertheless, **there are steps that can be taken by service providers and developers to improve their compliance posture**. The EDPB points out that the principle of data minimisation and data protection by design and by default should be carefully considered. [16]

4 Challenges of Covid, GDPR and Health Information

Health-related data under the GDPR is considered a special category of personal data, which requires a specific mandate in order for the processing to be compliant with data protection rules. Within the context of the legal grounds that are available, the processing of health data could be relied on the necessity for reasons of public interest in the area of public health, in accordance with the conditions of Art. 9 (2 (i)) GDPR, for healthcare purposes, under Art. 9 (2(h)) GDPR, and under certain conditions with explicit consent (Art. 9 (2(a)) GDPR). [17]

4.1 Findings from the Survey on Privacy of Health Information

As a result of the ongoing pandemic, the collection and use of health information became widespread[18]. For this reason, the survey contained questions related to the perception of citizens with regard to their health data during Covid-19.

From the results of the survey in this respect, **half of the respondents (52%) had concerns about the privacy of their health records**, while 38% did not have any concerns, and 10% did not know whether they had any concerns. It is clear that more respondents were worried about their health records, than not. In observing the number of individuals that had to provide health information to their employers, 70% did not have to. Although this is an encouraging percentage, there were different types of health information that employees had to disclose to their employer. On the one hand, some employees disclosed merely whether they were "fit for work". On the other hand, a number of employees stated that they had to disclose when they were infected by Covid-19, to provide a negative test of Covid-19, or to confirm that they are free of symptoms and had not been in contact with confirmed Covid-19 cases. While other respondents had to disclose their temperature or certain health information before entering the office. The most concerning privacy invasion observed was arguably the need to "report daily" their state of health, including fever, pains and Covid-19 related symptoms. In addition to the employment context, respondents were also asked whether they provided health information to other organisations. The majority of the respondents, and precisely 64%, did not provide health information to other organisations. Even so, the fact remains that **29% had to share health information with other organisations**.

The most concerning aspect of this section was a question on whether their doctor had adequately informed them on their data's cybersecurity, in which **4 in 5 respondents answered negatively (79%)**. The reason for the lack of adequate information on the cybersecurity of the respondent's data

[16] Paragraph 24 of European Data Protection Board Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak.

[17] Paragraph 33 of European Data Protection Board Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak.

[18] World Health Organisation, Covid-19 significantly impacts health services for noncommunicable diseases: available at: https://www.who.int/news/item/01-06-2020-Covid-19-significantly-impacts-health-services-for-noncommunicable-diseases.

is unclear. However, it **emphasises a lack of awareness of data protection by health professionals, and a clear need for training that focuses on delivering adequate information to patients** when it comes to health-related data. It seems improbable that doctors would have appropriate security measures implemented and would not mention these to their patients, especially during distressful times when privacy is at stake. Therefore, it can be inferred that appropriate security measures may be lacking entirely. The second recommendation that can arise **from this feedback is for cybersecurity tools and services to allow for customisation by health institutions in order to guarantee data protection to special categories of personal data** (such as health data, biometric data, and genetic data).

These concerns were expressed further on a broader question on other concerns the respondents may have had regarding their health data. One of the main issues was those hospitals, doctors and medical practitioners "do not care" about privacy, and do not have any "knowledge about IT and data security". A very frequent concern was that their health data could be used for commercial purposes, for example to analyse their eligibility for health insurance. Throughout the responses, this recurrent trend that the practices of health personnel are not up to date with the legislations on data protection compliance is worrisome. One respondent noted that "in most cases the [medical] systems are maintained by external service providers whose focus is on function and not security". This point goes hand in hand with the above recommendation **on the need for cybersecurity services that will have personal data as a main priority, by design and by default**. This will both support the health-care sector, by guaranteeing adequate security measures, as well as help, raise awareness on the need to inform patients about the security of their data, and how they can exercise their rights.

The last concern, which wraps up the aspect of security in the healthcare sector, is that of cybersecurity attacks. **Several participants in the survey mentioned ransomware attacks and that their repercussions are a major concern**. One participant from France mentioned that two months following surgery at a private clinic, they randomly found out that a hack had occurred in the clinic's network. The respondent demonstrated disappointment at not having been informed by the healthcare clinic directly, instead of the newspaper. Another respondent complements this point by explaining that ransomware attacks are used as means to blackmail data subjects' data on psychological treatments.

5 Challenges of Covid, GDPR and Personal Data Collection

The responses to Covid-19 have varied across the world, however, one similarity can be observed above all, that of “harnessing the power of data” to develop effective tools and measures.[19] Data collection has come at a turning point as both governments and private entities heavily rely on data access to ensure public safety and business continuity, respectively. [20] The GDPR can help ensure that any personal data processed in the context of the pandemic is done in a compliant, and lawful way.[21] This extensive data collection may introduce challenges that impact citizens, their perception of their privacy (or lack thereof), and their feelings towards entities processing their personal data.

5.1 Findings from the Survey on GDPR and Personal Data Collection

Following on from the above, an open question was asked on what the respondents' concerns were regarding personal data collection in the context of Covid-19. The responses varied from ideological concerns, to cybersecurity and privacy concerns. Some respondents stated that **their concern was**

[19] OCED Policy Responses to Coronavirus (COVID-19), Ensuring data privacy as we battle COVID-19, 14 April 2020, available at: https://www.oecd.org/coronavirus/policy-responses/ensuring-data-privacy-as-we-battle-covid-19-36c2f31e/ .
[20] OCED Policy Responses to Coronavirus (COVID-19), Ensuring data privacy as we battle COVID-19, 14 April 2020, available at: https://www.oecd.org/coronavirus/policy-responses/ensuring-data-privacy-as-we-battle-covid-19-36c2f31e/ .
[21] Statement on the processing of personal data in the context of the COVID-19 outbreak, Adopted on 19 March 2020, p.1, available at:
https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf .

sharing data with third parties. While several respondents' concern was **the use of their data for different purposes, the abuse of the initial purpose unintentionally, or further processing their data**. This concern is parallel to a violation of **purpose limitation**, whereby the GDPR states that any data controller must collect and process personal data for a specified, explicit and legitimate purpose. The voiced worries concerned both the legitimacy of the purpose - for example, violations to a legal processing of their tracking data, as well as the specified and explicit criterions of the principle. These concerns can be grouped towards **a broader risk of privacy relating to tracking apps**.

Along those lines, there were also worries regarding the **use of the tracking information to record their associated habits, routines and interests**. This could be considered a concern against them being profiled by the government or public authority. It is important to ensure that the citizens understand that the transparency of their applications is of utmost importance. It is worth noting that it seems some citizens believe that statistics and aggregated data analysis may consist of personal data, which by default is not the case. Another common concern among respondents was **cybersecurity-related attacks** that could compromise their privacy, freedom and physical security, such as maliciously collecting and processing their tracking data. This is in line with the above recommendation in which cybersecurity services can offer guarantees, namely, by ensuring that **an appropriate management of cybersecurity attacks is available to the healthcare systems**.

A less common concern was relating to the **violations of liberality and freedom**, which was also expressed as the tracking of border crossings and app proximity tracing. This considers the more ideological, constitutional and human rights concern of citizens' regarding their general freedom of movement. Interestingly, participants overwhelmingly noted that they feel that other apps could be tracking their movements too, including Google Maps, Google, Facebook, WhatsApp, LinkedIn and Instagram.

When respondents were asked whether they felt an increasing need to have control of their personal data during this time, an overwhelming majority (78%) responded positively. In addition, **60% of the respondents felt greater appreciation of the laws on privacy and data protection after the Covid-19** pandemic rolled out.

A major concern was the sharing of information with a third party, the use or abuse of such data for malicious ends. These concerns could be grouped in a broader context relating to tracking apps. This is in line with the above recommendation in which cybersecurity services can offer guarantees, namely, by ensuring that **an appropriate management of cybersecurity attacks is available to the healthcare systems**.

6 Challenges of Covid, Privacy and Transparency

The principle that has significant impact to the data subjects' perception of their privacy is that of transparency.[22] As mentioned in Section **Error! Reference source not found.**, under the GDPR's principle of transparency,[23] controllers are required to provide data subjects with clear information as to their activities involving the processing of personal data, under, e.g., Arts. 13 and 14 GDPR. The EDPB has re-emphasised the need for data subjects to receive transparent information during the pandemic, including the main features of the processing, the purposes and the retention period of the processing. [24] However, in the Covid-19 pandemic, as a result of the urgency of processing

[22] Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, p.6, available at: https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7 .

[23] Art. 5(1)(a) GDPR.

[24] Statement on the processing of personal data in the context of the COVID-19 outbreak, Adopted on 19 March 2020, p.2, available at:
https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf .

data, complying with regulations and implementing protection controls for protecting citizens nationally was very challenging.

6.1 Findings from the Survey on Privacy and Transparency

Interestingly, **almost half of the respondents now have higher expectations from privacy policies, as opposed to the time prior Covid-19**. Out of the 43% that now have higher expectations from privacy policies, thought-provoking recommendations have been suggested with regards to their expectations.

The most repeated response **suggested a higher need for clarity on the steps to exercise data subject rights**, as well as more straightforward ways to track data flows. This point also relates to the abovementioned need for more **interoperability** between tracking applications (for example, if one is under quarantine in Italy, if they travel to France, they can transfer the relevant data to the application used in France). However, the concentration on these type of expectations among participants suggests that guidance and clarity by cybersecurity services on the techniques, technical means and tools for exercising data subject rights is integral during the extraordinary times of the pandemic. Along these lines, another expectation mentioned was the ability to customize privacy settings. Thus, the feedback received from respondents **further increases the necessity for cybersecurity services to focus on appropriate means for data subjects to exercise their rights in the field of healthcare applications, software, as well as embed privacy settings customization, where possible**.

The second most common response asked for **enhancement and explanations of the safety measures**. This is another concerning point since it can be interpreted as a gap of comprehensible communications towards data subjects when it comes to the security of their data. As has been observed by the ENISA, malicious actors have been taking advantage of the pandemic to launch **phishing campaigns and ransomware attacks in the healthcare sector**.[25] One respondent specifically referred to the Covid-19 pandemic as a time where more private data was collected than before, and accordingly "a more sensitive handling of this data is required". The expectation of better explanations of the security measures may be due to the fact that data subjects consider the variable of Covid-19 as a reason for the collection of more sensitive type of personal data **and thus the need to understand the type of security measures is further highlighted.** In addition, another respondent pointed out that protection of the reputation of data subjects is integral during Covid-19, which further increases the expectations for appropriate security measures. More specifically, a respondent mentioned that the explanation of the "design of security measures" could be useful. Therefore, the mere inclusion of a list of security measures is not considered acceptable by data subjects during the pandemic. The recommendation that arises from this feedback is that **enhanced explanations of the implemented security measures within privacy policies is crucial**.

Another frequent response requested a **clearer explanation of privacy-related risks**. It can be observed that the risk-based approach of the GDPR remains important during the pandemic, also on the side of the data subjects. The privacy-related risks are exacerbated by the current pandemic, especially since the risks that could materialize could be unlike what the data subjects may be more familiar with, both in terms of their nature and consequences. One respondent expressed the need to protect the reputation of the data subjects. Linked with this concern is the expectation for "non-invasive privacy by default". The cybersecurity services can be of assistance, by offering privacy by default to the healthcare systems, software, and applications used. The recommendations towards the stakeholders are to ensure that **privacy-related risks are explicitly communicated to the data subjects**. In addition, cybersecurity tools and services can use privacy by default as a vehicle to both carry out a proper risk-assessment of the processing activities in the healthcare sector, as well as explaining the said privacy risks to the data subjects.

[25] European Agency on Cybersecurity, Cybersecurity in the healthcare sector during Covid-19 pandemic.

7 Related Cyberwatching.eu Publications

- Emerging technologies in the age of GDPR – Findings & recommendations from EU & R&I projects[26]
- Cybersecurity risk management: How to strengthen resilience and adapt in 2021[27]
- Security and Privacy by Design for Healthcare[28]

[26] https://cyberwatching.eu/publications/emerging-technologies-age-gdpr-%E2%80%93-findings-recommendations-eu-ri-projects
[27] https://cyberwatching.eu/publications/cybersecurity-risk-management-how-strengthen-resilience-and-adapt-2021
[28] https://cyberwatching.eu/publications/security-and-privacy-design-healthcare

cyberwatching.eu has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740129.