cyberwatching.eu
The European watch
on cybersecurity & privacy

Cybersecurity and data protection challenges in the Internet of Things (IoT)

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

1 Introduction 3
2 Challenges of Data Minimisation 3
3 Challenges of Data Processing Roles 5
4 Challenges of Purpose Limitation 7
5 Challenges of Transparency and Lawfulness 7
6 Challenges of Security 9
7 Related Cyberwatching.eu Publications 10

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

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.[1] Considering that the European Union Agency for Cybersecurity (ENISA) has identified IoT as a 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*",[2] ensuring that appropriate security measures can be defined for IoT systems is a matter of particular concern.

2 Challenges of Data Minimisation

IoT devices and services, as they are generally currently designed, inherently require the processing of large amounts of data (including personal data).[3] 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,[4] 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,[5] this creates a **conflict with the GDPR's principle of data minimisation**. As noted by the Article 29 Data Protection Working Party, "*[]some 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*".[6]

One solution which could be considered by IoT developers/providers is to **more comprehensively design 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.[7] 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*

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] See Section 3.1.1, above.

[6] 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.

[7] 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*".

service run on the IoT, the data subject should at the least be offered the possibility to use the service anonymously".[8]

The **European Data Protection Board** (**EDPB) has produced recent guidelines which can act as a helpful checklist in this regard**, particularly concerning the principle of data minimisation.[9] 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'[10] or 'privacy interfaces' for individuals[11]** – 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.[12] **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.[13]**

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.**[14]

[8] 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.

[9] 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/.

[10] 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. 20-22.

[11] 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/.

[12] 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.

[13] 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.

[14] 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.

3 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.[15] 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.[16]

Given the variety of data processing roles which these stakeholders may play (which may vary per activity),[17] 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 controllership[18] 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.

In particular, the **GDPR does not provide any express obligations to contractually regulate instances where stakeholders may be acting as autonomous controllers**,[19] 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 with each other through more complex contractual frameworks** (which we would conventionally call "**Data Management Agreements**"), identifying the specific data processing activities/relationships which take place between them and their respective roles for each one,[20] and agreeing on different sets of terms to

[15] 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.

[16] 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 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.

[17] A data processing role should be defined for each specific data processing activity or operation performed by an organisation, and not merely adopted wholesale. Our practical experience has shown 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). 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, 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.

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

[19] 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).

[20] 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

regulate each category of activity/relationship: (1) controller-to-processor terms, including the minimum obligations of Art. 28(3) GDPR,[21] (2) joint-controllership terms, including the minimum requirements of Art. 26 GDPR,[22] 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**.

collaborative economy (16 December 2015, available at: https://edps.europa.eu/sites/edp/files/publication/15-12-16_online_platforms_en.pdf), p. 5.

[21] 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).

[22] 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.

4 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, "*in 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*".[23] The 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*".[24] In this sense, similarly to AI, 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, 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) 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**.

5 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.[25] 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.[26] 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 on by IoT developers, such as consent[27], as well as the ability for individuals whose data is processed to

[23] 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.

[24] 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.

[25] 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

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

[27] 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.

exercise their rights under the GDPR (as, without knowledge that a processing activity is going on, this becomes impossible). As noted above, this runs afoul of the GDPR's principle of transparency, and of the concrete obligations to provide information to data subjects within the GDPR.[28] The GDPR requires information on data processing to be served to individuals before processing happens,[29] thereby reinforcing traditional and time-bound conceptions of notice.[30]

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 notifications[31] and periodic notifications,[32] 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.[33]**

Furthermore, **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.**

[28] Arts. 12, 13, 14, 15 and 34 GDPR.

[29] 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.

[30] 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.

[31] 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.

[32] Jennifer Kashatus, *Building Privacy into the Internet of Things* (4 August 2015), available at: https://www.technologyslegaledge.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.

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

6 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.[34] 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.[35] 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.[36] 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 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.[37] 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.[38] Furthermore, an additional consideration would be the **implementation of end-to-end encryption regarding all data collected and transmitted by and between IoT-connected devices and services.[39]** Further

[34] 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. 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.

[35] 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.

[36] 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.

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

[38] 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.

[39] 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. 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.

security measures and best practices which should be considered include those within **ENISA's guidelines on Good Practices for Security of Internet of Things.**[40]

7 Related Cyberwatching.eu Publications

- Emerging technologies in the age of GDPR – Findings & recommendations from EU & R&I projects[41]
- Decentralized operation and security in the IoT Space[42]

[40] 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.

[41] https://cyberwatching.eu/publications/emerging-technologies-age-gdpr-%E2%80%93-findings-recommendations-eu-ri-projects

[42] https://cyberwatching.eu/publications/decentralized-operation-and-security-iot-space

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