CARISMAND
Culture And RISk management in
Man-made And Natural Disasters

H2020-DRS-21-2014

HORIZON 2020 PROGRAMME

Secure societies – Protecting freedom and security of Europe and its citizens

Collaborative and Support Action

Grant Agreement Number 653748

CARISMAND

Culture And RISk management in Man-made And Natural Disasters

Citizens' rights

Lead Partner – P6 LUH

D6.4 – Recommendations on privacy friendly disaster management

30 June 2018

Project co-funded by the European Commission within the Horizon 2020 Programme (2014-2020)		
Dissemination Level:		
PU	Public	x
CO	Confidential, only for members of the consortium (including the Commission Services)	
EU-RES	Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)	
EU-CON	Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)	
EU-SEC	Classified Information: SECRET UE (Commission Decision 2005/444/EC)	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

Document Version Control:		
Version 0.1	Originated by: Iheanyi Nwankwo and Kai Wendt	On 31/01/2018
Version 0.2	Revised by: Iheanyi Nwankwo and Kai Wendt	On 15/06/2018
Version 0.3	Reviewed by: Saleh Al-Sharieh	On 22/06/2018
Version 0.4	Reviewed by: LIF Team	On 27/06/2018
Version 0.5	Reviewed by: Iheanyi Nwankwo	On 29/06/2018

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

Abbreviations

BCR	Binding Corporate Rules
CFREU	Charter of Fundamental Rights of the European Union
CdF	Municipality of Florence
CoE	Council of Europe
DPA	Data Protection Authority
DPD	Data Protection Directive
DPIA	Data Protection Impact Assessment
EC	European Commission
EU	European Union
ECtHR	European Court of Human Rights
ECHR	European Convention on Human Rights
e-IDAS	electronic IDentification, Authentication and trust Services
EDPS	European Data Protection Supervisor
ESOs	European Standardisation Organisations
EMSC	European-Mediterranean Seismological Centre
ENISA	European Union Agency for Network and Information Security
GDPR	General Data Protection Regulation
ISO	International Organization for Standardization
ICRC	International Committee of the Red Cross
IT	Information Technology
LED	Law Enforcement Directive
NGO	Non-Governmental Organisations
PLV	Valencia City Council-Local Police
PETs	Privacy Enhancing Technologies
PBD	Privacy by Design
PITs	Privacy Intrusive Technologies
SPoC	Single Point of Contact
SDM	Standard Data protection Model
STS	Special Telecommunications Service
SYP	South Yorkshire Police
UNCESCR	United Nations Committee on Economic, Social and Cultural Rights
UN	United Nations
UNHCR	United Nations High Commissioner for Refugees
UK	United Kingdom

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

Executive Summary

This deliverable evaluates existing privacy by design and privacy by default approaches in disaster management and delivers a set of non-technical and technical recommendations on how to strengthen citizens' privacy rights in daily routines of disaster managers and practitioners without risking the efficiency of disaster management mechanisms. This task directly feeds the toolkit in the area of citizens' fundamental rights.

This report first looks at the nature of personal data processing in disaster management and how the data protection principles apply to such circumstances. The principle of privacy by design and by default is then analysed within the broader context of the information system used for processing personal data. Several legal sources imposing the obligation of privacy by design, as well as guidelines and strategies for its operationalisation were discussed. Examples of how some disaster management organisations have implemented privacy by design in their policies were shown, indicating a divergence in implementation strategies. The final part of this report contains the recommendations.

These recommendations are informed, in general, by the output of the previous tasks in this work package, and in particular, the interpretation of data protection principles, and the principle of data protection by design and by default under the European Data Protection Law by data protection authorities, as well as other important national and EU institutions. The recommendations are addressed to policymakers and disaster managers. In a nutshell, they include non-technical recommendations such as:

1 Policymakers and disaster managers to adopt an overarching rights-based approach in disaster policies and operations.
2 Relevant authorities to support and promote research and development in the area of privacy-friendly software and systems used in disaster management.
3 Relevant authorities to develop and publish guidelines on privacy and data protection in disaster and other emergency management.
4 Disaster managers to establish coherent and transparent privacy and data protection policy.
5 Relevant stakeholders to define specific rules on how to operationalise and achieve data protection by design and by default.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

6 Disaster managers to carry out a data protection impact assessment before initiating a new data processing system.

7 Disaster managers to incorporate regular training programme on privacy, data protection and data security as part of the management activities.

8 Disaster managers to anticipate innovative technology and leverage its potential for data protection.

9 Disasters managers and practitioners to further research on instruments and practices relating to cultural rights in disaster management, develop operational guidelines and practice directives, and integrate modules on cultural competencies for training purposes.

10 Disaster managers to foster a proactive strategy of consultation with cultural stakeholders or communities and citizen awareness.

And technical recommendations such as:

11 Policymakers to develop a common infrastructure, based on state of the art IT-Security principles for use in disaster management.

12 Disaster managers to implement relevant standards, code of conducts or certification relating to information system management to enhance privacy and data protection.

13 Where possible, for disaster managers to develop and provide own technical solutions for an effective and privacy-friendly disaster management and host information systems in a secure environment.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

1.0 Introduction

The nature of disaster management (prevention, response, recovery operations) makes it inevitable to process personal data, either involving the public, disaster victims and/or the disaster management personnel and volunteers. Data processing here could range from processing manual files such as recording names of refugees at the border crossing to in-house IT-systems or cloud deployments, to apps that notify the public of disaster incidents or forecast. It is, therefore, not surprising that the EU General Data Protection Regulation (GDPR) also addresses issues of data processing in disaster situations.[1] Similarly, where the occurrence of a disaster threatens public security, it could trigger the application of Directive 2016/680 on processing personal data for law enforcement purposes (Law Enforcement Directive – (LED).[2] For instance, when dealing with terrorism (considered as a disaster) or when the processing activities are related to the prevention or investigation of the terrorist act, the LED provides the legal basis. Other national legislation such as those regulating the police could also have an impact on the processing of personal data in disaster cases. Thus, it could be said that data processing in a disaster situation is regulated in the EU.

However, there has been an instance where compliance with data protection laws has tended to hinder or delay disaster operations in the absence of a well-defined framework. In the wake of the bombing incident in the UK in 2007, there was confusion whether data protection principles should apply in such emergency, and this was identified as one of the factors that hampered or delayed the connection of survivors to support services.[3] Similar situations have also been

[1] See 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 - GDPR), recitals 46 and 73.
[2] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive).
[3] HM Government, *Data Protection and Sharing – Guidance for Emergency Planners and Responders* (HM Government 2007) 5 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60970/dataprotection.pdf> accessed 24 March 2018.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

witnessed in Australia and New Zealand,[4] thereby requiring clear and specific rules on the application of data protection principles in disaster or emergency scenarios.

The GDPR is a European regulation of general application, and its principles, obligations, and rights apply in disaster management. One of such principles is the principle that the protection of personal data shall be a default characteristic of information systems, and this is captured in the obligation of data controllers to implement data protection by design and by default.[5] Such obligation implies that data controllers must implement the data protection principles, as well as technical and organisational measures to secure the personal data under their care right from the design stage of their information processing systems.

However, there is no consensus as to how to operationalise these data protection principles or the holistic concept of privacy by design in the system design. Earlier propositions for using technological mechanisms for safeguarding privacy-related interests were coined under the notion of privacy-enhancing technologies.[6] It is this philosophy of using technology that threatens privacy to safeguard privacy interests as well that metamorphosed into the notion of privacy by design, a concept that centres on embedding privacy consideration into the design specifications of technologies that process personal data or could affect privacy in general.[7] Since its inception, there have been various suggestions and approaches on how to operationalise the concept, yet, the debate continues among privacy engineers and practitioners considering the diversity of information systems that process data.

Ann Cavoukian, one of the earliest proponents of privacy by design, suggests that 'privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organisation's default mode of operation.'[8] Such position according to Bygrave implies recognition of 'the ability of information systems architecture to shape human conduct in

[4] Reidenberg J et al., Privacy and Missing Persons after Natural Disasters (Center on Law and Information Policy at Fordham Law School and Woodrow Wilson International Center for Scholars 2013).
[5] There are other data protection instruments that also impose the obligation of data protection by design and by default such as the Law Enforcement Directive. The proposal for a reform of the e-Privacy Directive also considers this principle.
[6] This notion was brought to limelight by a report of a joint project set up by the Dutch Data Protection Authority and the Ontario Information Commissioner. See Ann Cavoukian, *Privacy by Design… Take the Challenge* (Ontario 2009) <https://web.archive.org/web/20120119044635/http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf> accessed 24 March 2018.
[7] Lee Bygrave, 'Hardwiring Privacy' University of Oslo Faculty of Law Research Paper No. 2017-02.
[8] Ann Cavoukian 'Privacy by Design: The 7 Foundational Principles' (2009, revised 2011) <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf> accessed 24 March 2018.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

ways that parallel the imposition of law laid down by statute and contract, and to shape conduct more effectively than such law.'[9] This can only be realised by building the fundamental principles of data protection into the design, operation and management of information processing technologies and systems.

Although as originally conceived, the notion of privacy by design applied to information technology, Cavoukian sees prospects in expanding the scope to business practices, and physical design and infrastructures.[10] She also notes that the broad concept of privacy by design encompasses many elements in practice,[11] and further develops seven fundamental privacy by design principles (see further discussion in Section 3.2.2). [12] However, these initial efforts did not stop debates surrounding the practical implementation and methodology of operationalising privacy by design. Some critics argue that the concept and its principles have fallen considerably short of delivering 'the answer' that the proponents envisaged. Bygrave attributes a wide array of factors to this shortfall such as the fact that the notion is 'at odds with powerful business and state interests, and simultaneously remains peripheral to the concerns of most consumers and engineers.'[13]

These criticisms notwithstanding, there is a prospect that by making data protection by design and by default obligatory under the GDPR, the attitude of data controllers will change. The ability to show that all the tests and reviews necessary to ensure privacy compliance from the design stage of a product or system will be crucial in the future. This is especially so in the light of the accountability and transparency principles of the GDPR, and the expectation that data controllers must facilitate the exercise of the data subjects' rights from the beginning.[14]

Thus, considering privacy implications associated with disaster management, it is essential to define specific rules on how to achieve data protection by design and by default in disaster

[9] Bygrave (n 7) 2.
[10] Cavoukian (n 8).
[11] These elements are:
1. Recognition that privacy interests and concerns must be addressed;
2. Application of basic principles expressing universal spheres of privacy protection;
3. Early mitigation of privacy concerns when developing information technologies and systems, across the entire information life cycle;
4. Need for qualified privacy leadership and/or professional input; and
5. Adoption and integration of privacy-enhancing technologies (PETs). Ibid.
[12] Cavoukian (n 8).
[13] Bygrave (n 7) 3.
[14] Article 29 Working Party, Guidelines on Transpareny under Regulation 2016/679, WP 260. <http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850> accessed 2 April 2018.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

information management systems. This would help disaster managers to translate legal requirements into practical controls and appropriate safeguards. To do so, however, it is important to have a clear understanding of how IT-systems are designed for data processing in general, and disaster management in particular. Such analysis would provide more insight into the current practices and the extent to which privacy by design and by default and other privacy enhancing technologies (PETs) have been or need to be embedded into disaster management systems and policies.

2.0 Methodology

Desk research on privacy by design was conducted focusing on primary and secondary EU law, as we all as published literature in this area including opinions and guidelines from data protection authorities and reputable EU and national institutions. Information on how disaster information systems implement privacy by design and by default is gathered through a short survey of the project partners who work in the disaster management field. Responses were received from four partners who work in this field, namely, South Yorkshire Police (SYP), UK; Municipality of Florence (CdF), Italy; Valencia City Council-Local Police (PLV), Spain; Special Telecommunications Service (STS), Romania; and one partner who only produces services and products that can be used in disaster management – European-Mediterranean Seismological Centre (EMSC), France. A sample of the survey is annexed to this deliverable.

3.0 Key Concepts and Implementation

3.1 Definition of key concepts

Privacy by Design (PBD) is often interchangeably referred to as **Data Protection by Design** in many instances, although some commentators argue that both terms are not completely synonymous.[15] This distinction is made clearly in the recent preliminary opinion of the European Data Protection Supervisor (EDPS) who uses the term "privacy by design" to designate the broad concept of technological measures for ensuring privacy as it has developed in an international

[15] Bygrave (n 7).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

debate over the last few decades, while using the terms 'data protection by design' and 'data protection by default' to designate the specific legal obligations established by Article 25 of the GDPR.[16] Subtle as this demarcation might be, common usage and application of both terms, however, suggests that they convey a similar meaning, especially, regarding the measures undertaken to achieve them. There is no universally accepted definition of both terms, and none of the data protection instruments at the EU-level defines either of the terms. In this deliverable, both terms are used in tandem.

Klitou provides a general definition of privacy by design as follows:

> PBD is the realisation of values, in this case, the principles of privacy and corresponding rules/regulations, via the physical design, technical specifications, architecture and/or computer code of the device, system or technology concerned, where applicable. The aim of PBD is to design and develop a system or device (i.e. software and/or hardware) in a way that supports and materialises those privacy principles, values and rules as goals and functions, whereby that system or device then becomes 'privacy-aware' or 'privacy-friendly'. In other words, PBD can be defined as practical measures, in the form of technological and/or design-based solutions, aimed at bolstering privacy/data protection laws, better ensuring or almost guaranteeing compliance, and minimising the privacy-intrusive capabilities of the technologies (i.e. PITs) concerned.[17]

This definition appears all-encompassing, pointing to many aspects of the concept—its goals, means of achievement, and methodology. Cavoukian also defines privacy by design 'as an engineering and strategic management approach that commits to selectively and sustainably minimise information systems' privacy risks through technical and governance controls.'[18] In essence, privacy by design reflects a systematic approach to ensure that due consideration is given to privacy-related interests from the earliest conception of the data processing system (during the design of the system) through to the entire lifecycle of the data processing operation.

Article 25 of the GDPR requires from the data controllers both at the time of the determination of the means for processing and at the time of the processing itself, to implement appropriate technical and organisational measures, which are designed to implement data protection principles, in an effective manner and to integrate the necessary safeguards into the processing

[16] EDPS, Opinion 5/2018 Preliminary Opinion on privacy by design, (31 May 2018) 1.
[17] Demetrius Klitou, 'A Solution, But Not a Panacea for Defending Privacy: The Challenges, Criticism and Limitations of Privacy by Design' in Bart Preneel and Demosthenes Ikonomou (eds), *Privacy Technologies and Policy: First Annual Privacy Forum, APF 2012* (Springer Verlag 2014) 86.
[18] Ann Cavoukian, *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices* (Ontario 2012).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

for the protection of the data subjects' rights. The EDPS has identified four dimensions of the obligation of data protection by design as follows: (1) consideration of safeguards both at the design and operational phase, and clearly identifying the protection of individuals and their data within the project requirements, (2) adopting a risk management approach (3) implement measures appropriately and effectively and (4) integrate the identified safeguards into the processing.[19]

Another important concept associated with privacy by design is **Privacy by Default**. Cavoukian explains privacy by default in these words:

> We can all be certain of one thing − the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy − it is built into the system, by default.[20]

The Irish Computer Society also states that privacy by default means that once a product or service has been released to the public, the strictest privacy settings should apply by default, without any manual input from the end user.[21] ENISA addressed privacy by default, in particular, by stressing the data minimisation principle,[22] also highlighting the practical force and importance of the default settings for the end-users' enjoyment of privacy. As such, whenever default settings are pre-configured, they must be carefully chosen so that only personal data which are necessary for each specific purpose are processed.[23]Article 25 (2) of the GDPR covers data protection by default. In essence, privacy by default requires that the defaulting setting of the information processing system be privacy oriented, and the approach continues throughout the life cycle.[24]

In recent times, the concept of **security by design and by default** has also emerged, referring to a situation where the security aspect of an information system security is considered right

[19] EDPS, Opinion 5/2018, 6-7.
[20] Cavoukian (n 8).
[21] ICS, 'What is Privacy by Design & Default? <https://www.ics.ie/news/what-is-privacy-by-design-a-default> accessed 2 April 2018.
[22] ENISA, *Privacy and Data Protection by Desgin – from policy to engineering* (ENISA 2014) 5 <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design> accessed 12 April 2018.
[23] ENISA, *Privacy and Data Protection in Mobile Applications* (ENISA 2017) < https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications> accessed 12 April 2018.
[24] See Lee Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements', Oslo Law Review, Vol. 4 No.2, 2017.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

from the start and built-in the design of the system so that by default the system is adjudged secure. It is a systematic approach to ensure security; instead of relying on auditing security in a retrospective. [25] The concept provides developers with the ability to build security control in throughout the development process and the life cycle of the system. It begins with taking a more proactive approach to information system security and does not rely on the typical protective or reactive third-party security tools; rather, it builds security into the infrastructure from the ground up.[26] End-to-End security is one notion that exemplifies this concept, implying that security protocols are implemented on the endpoints of a connection (client-server, or client-client for peer-to-peer) for secure communications from one end system or device to another.[27] Encryption, anonymisation, psuedonymisation, etc., are also examples of techniques that ensure the security of data.

Data Protection Impact Assessment (DPIA), although not defined in the GDPR, the European Commission has referred to it as "a process whereby a conscious and systematic effort is made to assess privacy risks to individuals in the collection, use and disclosure of their personal data. DPIAs help identify privacy risks, foresee problems and bring forward solutions."[28] Also, in the Smart Meter recommendation, the Commission called it "a systematic process for evaluating the potential impact of risks where processing operations are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes to be carried out by the controller or processor, or the processor acting on the controller's behalf".[29]

In essence, DPIA is seen as a proactive risk management tool for discovering and assessing the risks that personal data may face while undergoing processing, as well as to bring forth solutions

[25] AET, 'Security by Design and Secure by Default' (10 May 2017) <https://www.aeteurope.com/news/security-design-secure-default/> accessed 14 April 2018.
[26] Ibid.
[27] Michael H. Behringer, 'End-to-End Security' *The Internet Protocol Journal,* Vol 12, No.3 <https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-45/123-security.html>; Symantec, 'Compliance, "the Privacy by Design" Approach to Protect Personal Data' <https://www.comparex-group.com/MediaLibrary/Catalog/web/content_files/Presse/medial-pool/social/WHITEPAPER_Symantec_GDPR_2017.pdf> accessed 14 April 2018.
[28] Commission Staff Working Paper Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) SEC(2012) 72 final, i.
[29] Commission Recommendation of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems (2014/724/EU).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

to those risks through among other things by designing the systems in a privacy-friendly way. It covers all aspects of personal data processing, ranging from collection to disposal, and it is intended not to be just an exercise of ticking a checklist or a mere compliance check as the purpose, necessity and proportionality of the data processing must be reasoned in the process.

This is emphasized in the Article 29 Working Party guidelines on DPIA, which defines it as: "a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them."[30] In this respect, a DPIA should be able to analyse the security controls needed to mitigate various risks potentially facing the processing.

3.1 Legal Grounds of Privacy by Design

There are several legal grounds for implementing privacy by design. Although the Data Protection Directive (DPD) does not explicitly use the term privacy by design, some of its provisions reflect the practical intent of the concept, at least, regarding data security. For example, Recital 46 of the DPD requires the implementation of appropriate technical and organisational measures both at the time of the design of the processing system and at the time of the processing itself, which is further buttressed in Article 17 of the DPD focusing on data security. It is noteworthy, however, that some national laws implementing the Directive considered privacy by design more explicitly as seen, for example, in Section 3a of the German Federal Data Protection Act that implemented the Directive.[31]

The European Commission, the Article 29 Working Party and the European Data Protection Supervisor have all made several policy pronouncements recommending privacy by design.[32] The judiciary has also made pronouncements that have an impact on the subject of privacy by design. The effect of the ruling in the famous Google Spain case, for example, is that Google (and,

[30] Article 29 Working Party 'Guidelines on Data Protection Impact Assessment (DPIA)' Wp248rev.01, 4.
[31] It provides: "Personal data are to be collected, processed and used, and processing systems are to be designed in accordance with the aim of collecting, processing and using as little personal data as possible. In particular, personal data are to be aliased or rendered anonymous as far as possible and the effort involved is reasonable in relation to the desired level of protection."
[32] See for example: 'EDPS opinion on privacy in the digital age: "Privacy by Design" as a key tool to ensure citizens' trust in ICTs', <https://edps.europa.eu/press-publications/press-news/press-releases/2010/edps-opinion-privacy-digital-age-privacy-design_en>; the smart meter recommendation, etc.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

indirectly, other search-engine operators) must reconfigure the systemic aspects of its search-engine operations so that they are more privacy-friendly.[33]

The GDPR and the Law Enforcement Directive have significantly reformed the legal basis and implementation of privacy by design. It is now mandatory for data controllers to implement data protection by design and by default following Article 25 of the GDPR which provides:

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons

It is important to note that Article 25(1) mentions that appropriate technical and organisational measures should be designed to implement data protection principles which are contained in Article 5 of the GDPR—the lawful, fair and transparent processing; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability principles. Article 25(1) also indicates the criteria for assessing the implementation of data protection by design—effectiveness, safeguarding, compliant with the GDPR and protecting the rights of the data subjects. Article 5(2) equally indicates that data protection by default shall ensure that only personal data that is necessary for each specific purpose shall be processed (reflecting data minimisation principle). (See Section 3.2 for further discussion on these principles).

Once subtle criticism of Article 25 of the GDPR, however, is that it does not address manufacturers of information systems. In cases where it is not the data controllers that

[33] *Google Spain v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (CJEU 13 May 2014 in Case C-131/12).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

manufactures or designs the information systems, it may be late for them to incorporate data protection by design since the obligation is only addressed to them.[34] "Producers" are only encouraged under Recital 78 to take data protection by design and by default into account in their work. This may be difficult to enforce against such producers in practice. One remedy though, seen in the GDPR, is the requirement that data controllers shall not use technologies that collect more personal data than necessary, and shall engage only data processors that provide sufficient guarantee to implement appropriate technical and organisational measures. It is yet to be seen how this strategy will be implemented in the future.

Other sector-specific data protection laws also contain provisions on privacy by design. Article 20 of the Law Enforcement Directive imposes a duty on the competent authorities to implement data protection by design and by default like the provisions of the GDPR discussed above. The e-Privacy Directive, as well as the proposal for its reform, contain provisions on privacy by design. Recital 30 of the e-Privacy Directive, for example, recommends that 'Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum.'[35] Also, the e-IDAS Regulation provides that interoperability framework of the electronic identifications schemes shall facilitate the implementation of the principle of privacy by design.[36]

In practical terms, privacy by design should be considered as early as possible in the product/service design stage. This will be the same time that a DPIA is required according to the GDPR, enabling both tools to identify and assess the data privacy risks and challenges associated with the product, service or project, and suggest ways of building in mitigation of those risks into the architecture or design of the system, product, or process.[37] Thus, a DPIA appears to be an integral part of taking privacy by design approach. The results or outcomes of the DPIA should

[34] Bygrave (n 7) 18.
[35] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as amended. See also Recital 46. Note also that the proposal for reform of the e-Privacy Directive with a Regulation contains provisions aimed at privacy by design. This proposal is still undergoing negotiation.
[36] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Article 12 (3) (C).
[37] Peter Bolger and Jeanne Kelly 'Privacy by Design' (Lexology, 18 September 2017)
<https://www.lexology.com/library/detail.aspx?g=72cdafaa-9644-453c-b72c-3d55dc5dc29d> accessed 25 April 2018.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

be manifested or implemented through the privacy by design concept. As such, both tools are complementary; while a DPIA is used to uncover what is to be designed into the system for privacy protection, privacy by design and by default approach adopted by a system could be relied upon in the DPIA as a factor in the risk evaluation and mitigation process.[38]

3.2 Implementing Privacy by Design

3.2.1 The Relationship between Data Protection Principles and Privacy by Design

Data protection legislation contains basic principles for safeguarding the privacy of data subjects. These principles refer to general rules that express the fundamental obligations that all those processing personal data should observe.[39] They provide an overarching framework that guides data controllers and processors to develop an appreciation of the core goals of the regulatory intent, and at the same time, gives them the opportunity to find the most efficient ways of achieving the outcome required.[40] The ISO 29100:2011 *Information technology—Security techniques—Privacy framework*, defines privacy principles as a set of shared values governing the privacy protection of personally identifiable information (PII) when processed in information and communication technology systems.

Commentators argue that the target of privacy by design should be to fulfil the data protection principles. As the Norwegian DPA, for example, remarks, "Data protection by design and by default helps ensure that the information systems we use fulfil […] data protection principles, and that the systems safeguard the rights of data subjects".[41] This statement points to the close relationship between these fundamental principles and the concept of privacy by design.[42]

[38] For example, adopting measures such as pseudonimisation and anonymization which are instances of privacy by design could be considered as a risk mitigating factor in a DPIA.
[39] Australian Law Reform Commission, 'Regulating Privacy' *Australian Privacy Law and Practice* (ALRC Report 108, 2008); ISO 29100:2011 defines privacy principles as set of shared values governing the privacy protection of personally identifiable information (PII) when processed in information and communication technology systems.
[40] Australian Law Reform (n 39).
[41] Datatilsynet, 'Guide: Software development with Data Protection by Design and by Default' <https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/?print=true> accessed 23 May 2018.
[42] This relationship is also reflected in the GDPR, Article 25 (1) discussed earlier.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

Article 5 of the GDPR contains data protection principles, which are amplified in several other provisions of the GDPR. In a nutshell, these principles are summarised as follows:

1. **Lawfulness, fairness and transparency:** This principle comprises three in one. Lawfulness implies that data controllers must have legitimate grounds for processing personal data, and not use the data in ways that have unjustified adverse effects on the individuals concerned. For personal data processing to be lawful, the GDPR provides certain legal bases, which the data controller could rely upon—consent, performance of contract, compliance with legal obligation, protection of the vital interest of the subject or another natural person, performance of public interest task, and legitimate interest of the controller or third party.[43] Fairness implies that personal data must be processed fairly. This is important when conducting a balancing of interests test between the interests of the data subjects and that of the data controllers or other third parties. Transparency indicates that data must be processed in a transparent manner considering the data subject. This implies that data controllers must provide the data subjects with certain information about how they intend to use the data, and give individuals appropriate privacy notices when collecting their data.[44] Transparency, as the Article 29 Working Party explains, is an overarching obligation applying to three central areas under the GDPR: (1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and (3) how data controllers facilitate the exercise by data subjects of their rights.[45]
2. **Purpose limitation:** The principle of purpose limitation has two cornerstones: personal data must be collected for "specified, explicit and legitimate" purposes (purpose specification) and not be "further processed in a way incompatible" with those purposes (compatible use).[46] Specification of purpose is essential to identifying the legitimacy, applicable law for a particular data processing operation, as well as setting the limits for the data processing. This means that the purpose must be determined before commencing the data processing. However, the further use of data for compatible purposes is allowed on the ground of the initial legal basis in certain cases. Article 5(1)(b) provides instances of compatibility: 'further processing for

[43] See GDPR, Article 6 (1).
[44] ICO, 'Guide to Data Protection' <https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/>
[45] Article 29 Working Party (n 14).
[46] Art. 29 Working Party Opinion 03/2013 on Purpose Limitation, 00569/13/EN WP 203; GDPR, art. 5 (1) (b).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes'. Thus, further processing of retrospective data for compatible purposes (e.g., for scientific or historical research purposes or statistical purposes) is lawful and does not require another legal basis than that which allowed the initial collection.[47] However, appropriate safeguards must be implemented such as pseudonymisation and anonymisation where necessary to protect the data subjects.[48]

3. **Data minimisation:** Data minimisation is an important principle of data protection that must be taken into consideration when collecting data. This principle, as stipulated in Article 5(1)(c), states that personal data shall be adequate, relevant and limited to what is necessary for the purposes for which it is processed. Although the GDPR does not define "adequate and relevant" data, in effect, it means collecting and holding only the minimum amount of personal data needed to fulfil a certain purpose. On the one hand, organisations should ensure that the personal data they collect is adequate and relevant for the purpose for which it is to be processed, and on the other hand, should minimise the amount of data they collect and process for only the fulfilment of the identified purpose. As a corollary, data that is no longer needed must be deleted.
4. **Accuracy:** The accuracy principle means that personal data processed shall be accurate and, where necessary, kept up to date. This implies that the data controller shall use every reasonable step to ensure that personal data that is inaccurate is erased or rectified.[49] This principle is clear and evokes no much controversy as to operationalising it. In practical terms, it demands that the data controller must assess with reasonable care that the data is accurate and up to date.
5. **Storage limitation:** This principle is meant not to keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes of the data processing. Upon expiration of that period, data must be deleted or anonymised. Personal data may be stored for longer periods solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to

[47] See GDPR, recital 50, art. 89.
[48] GDPR, art. 89.
[49] GDPR, art 5(1)(d).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

implementation of the appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.[50] The implication of this for data controllers is that a data retention policy has to be set out, and the data must not be stored beyond the period that is necessary for which it is collected. Longer storage has to be for any of the purposes stipulated in Article 5(1)(e), and appropriate safeguards must be implemented.

6. **Integrity and confidentiality:** This principle implies that personal data must be protected against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures.[51] This principle goes to the heart of securing the data, and introduces an obligation for the data controllers and processors to assess the risk faced by personal data undergoing processing under their care, and implement appropriate security for such data. Importantly, to review the measures regularly to ensure that they are up to date and effective. Thus, data controllers and processors must implement measures to ensure a level of security appropriate to the risks resulting from their data processing.[52] Such safeguards include the pseudonymization and encryption of personal data where necessary, as well as regular risk assessment to forestall the breach of confidentiality, integrity and availability, and to maintain the resilience of processing systems and services.
7. **Accountability:** The accountability principle requires that the data controllers show how they comply with the principles and obligations imposed by the GDPR. Data controllers and processor could demonstrate compliance in various ways depending on the complexity and nature of their data processing. These may include conducting a data protection impact assessment; documenting and creating a personal data inventory; implementing data protection by design and by default; developing a data privacy governance structure which may include appointing a Data Protection Officer; etc.[53]

Operationalising these principles in the course of designing data processing systems has been a subject of discussion, and various interpretations have emerged on the subject. Although over the years, privacy by design has developed its principles,[54] we will discuss in the subsequent

[50] GDPR, art 5(1)(e).
[51] GDPR, art 5(1)(f).
[52] See GDPR, art. 32.

[53] See the ICO Accountability and Governance, in the Guide to the General Data Protection Regulation <https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/accountability-and-governance/> accessed 23 April 2018.
[54] See Cavoukian (n 8).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

section, the various efforts that have been made at implementing data protection principles in practical terms.

3.2.2 Information Systems Development: Operationalising the Data Protection Principles and Rights of the Data Subjects by Design and by Default

As earlier pointed out, various suggestions and opinions have been issued on how to operationalise privacy by design. There is no consensus on the actual implementation approach. As Cavoukian succinctly puts it, 'The approach will vary depending upon the organisation, the technology and other variables. While there is no single way to implement, operationalise, or otherwise roll out a PbD-based system, taking a holistic approach is key.' Such situation is challenging, especially as there is hardly any one-size-fits-all action guidelines for system developers. Cavoukian agrees that privacy by design can be used to integrate fair information practices. She, however, proposes seven Foundational Principles that may be used to accomplished privacy by design objectives, which she summarises as follows:

1. Proactive not Reactive; Preventative not Remedial

   The Privacy by Design (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

2. Privacy as the Default Setting

   We can all be certain of one thing – the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by default.

3. Privacy Embedded into Design

   Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality – Positive-Sum, not Zero-Sum

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

5. End-to-End Security – Full Lifecycle Protection.

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved – strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.

6. Visibility and Transparency – Keep it Open

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. Respect for User Privacy – Keep it User-Centric

Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.[55]

It is important to note that the provision of Article 25 GDPR goes beyond the seminal conception of privacy by design by Cavoukian, and does not necessarily rely on the principles she developed. However, some critics say that these fundamental principles do not provide the nitty-gritty of what will be the maximum degree of designing privacy in the default, or how should the design and default resist circumvention attempts.[56]

The Conference of the Independent Data Protection Authorities of the Bund and the Länder initiated a common and practical approach to implement data protection requirements (which they tag data protection goals) by publishing Standard Data Protection Model (SDM) in 2016. This model provides objective mechanisms to transfer the German Data Protection requirements into technical and organisational measures. These requirements were structured in terms of seven protection goals (context-independent properties for IT systems): data minimisation, availability,

[55] Cavoukian (n 18) 12.
[56] Bygrave (n 7).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

integrity, confidentiality, transparency, unlinkability, and intervenability, which were used to generate a catalogue of technical and organisational measures.

The following shows how these goals are operationalised in the design of the data processing system (privacy by design approach) in the SDM:

Data Minimisation

The protection goal data minimisation can be achieved by:

- Reduction of collected attributes of the data subject,
- Reduction of processing options in processing operations,
- Reduction of possibilities to gain knowledge of existing data,
- Preference for automated processing operations (not decision-making processes),
- Implementation of automatic blocking and erasure routines; procedures for pseudonymisation and anonymisation,
- Rules to control processes for the change of procedures.

Availability

Typical measures to guarantee availability are:

- Preparation of data backups, process states, configurations, data structures, transactions histories etc., according to a tested concept,
- Protection against external influences (malware, sabotage, force majeure),
- Documentation of data syntax,
- Redundancy of hard- and software as well as infrastructure,
- Implementation of repair strategies and alternative processes,
- Rules of substitution for absent employees.

Integrity

Typical measures to guarantee integrity or to assess a breach of integrity are:

- Restriction of writing and modification permissions,
- Use of checksums, electronic seals and signatures in data processing in accordance with a cryptographic concept,
- Documented assignment of rights and roles,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

- Processes for maintaining the timeliness of data,
- Specification of the nominal process behaviour and regular testing for the determination and documentation of functionality, of risks as well as safety gaps and the side effects of processes,
- Specification of the nominal behaviour of workflow or processes and regular testing of the detectability respective determination of the current state of processes.

Confidentiality

Typical measures to guarantee confidentiality are:

- Definition of a rights and role concept according to the principle of necessity on the basis of identity management by the controller,
- Implementation of a secure authentication process,
- Limitation of authorised personnel to those who are verifiably responsible (locally, professionally), qualified, reliable (if necessary with security clearance) and formally approved, and with whom no conflict of interests may arise in the exercise of their duties,
- Specification and control of the use of approved resources, in particular, communication channels,
- Specified environments (buildings, rooms) equipped for the procedure,
- Specification and control of organisational procedures, internal regulations and contractual obligations (obligation to data secrecy, confidentiality agreements, etc.),
- Encryption of stored or transferred data as well as establishing processes for the management and protection of the cryptographic information (cryptographic concept),
- Protection against external influences (espionage, hacking).

Unlinkability

Typical measures to guarantee unlinkability are:

- Restriction of processing, utilisation and transfer rights,
- In terms of programming, omitting or closing of interfaces in procedures and components of procedures,
- Regulative provisions to prohibit backdoors as well as establishing quality assurance revisions for compliance in software development,
- Separation in organisational / departmental boundaries,
- Separation by means of role concepts with differentiated access rights on the basis of an identity management by the responsible authority and a secure authentication method,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

- Approval of user-controlled identity management by the data processor,
- Using purpose specific pseudonyms, anonymisation services, anonymous credentials, processing of pseudonymous or anonymous data,
- Regulated procedures for purpose amendments.

Transparency

Typical measures to guarantee transparency are:

- Documentation of procedures, in particular including the business processes, data stocks, data flows and the IT systems used, operating procedures, description of procedure, interaction with other procedures,
- Documentation of testing, approval and, where appropriate, prior checking of new or modified procedures
- Documentation of the contracts with internal employees; contracts with external service providers and third parties, from which data are collected or transferred to; business distribution plans, internal responsibility assignments,
- Documentation of consents and objections,
- Logging of access and modifications,
- Verification of data sources (authenticity),
- Version control,
- Documentation of the processing procedures by means of protocols on the basis of a logging and evaluation concept,
- Consideration of the data subject's rights in the logging and evaluation concept.

Intervenability

Typical measures to guarantee intervenability are:

- Differentiated options for consent, withdrawal and objection,
- Creating necessary data fields, e.g. for blocking indicators, notifications, consents, objections, right of reply,
- Documented handling of malfunctions, problem-solving methods and changes to the procedure as well as to the protection measures of IT security and data protection,
- Disabling options for individual functionalities without affecting the whole system,
- Implementation of standardised query and dialogue interfaces for the persons concerned to assert and/or enforce claims,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

- Traceability of the activities of the controller for granting the data subject's rights,
- Establishing a Single Point of Contact (SPoC) for data subjects,
- Operational possibilities to compile, consistently correct, block and erase all data stored about any one person.[57]

Although this model was primarily designed with the German data protection framework in mind, a possible transposition with the GDPR's data protection principles was also included in the document.[58] However, there are still other approaches to the implementation of privacy by design in the EU such as by ENISA. Many academics have also written on the subject.[59] Below we highlight a few of them.

ENISA's Guidelines

ENISA first published *Privacy and Data Protection by Design – from policy to engineering* in 2014 where it tried to bridge the gap between the legal framework and the available technical implementation measures by providing privacy design strategies.[60] In this publication, ENISA, among other things, elaborated on eight privacy by design data-oriented strategies, and the design patterns towards implementing them. These strategies include,

1. MINIMISE: requires that the amount of personal data that is processed should be restricted to the minimal amount possible.
2. HIDE: requires that any personal data, and their interrelationships, should be hidden from plain view.
3. SEPARATE: requires that personal data should be processed in a distributed fashion, in separate compartments whenever possible.
4. AGGREGATE: requires that personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful.
5. INFORM: This strategy corresponds to the important notion of transparency and requires that the data subjects should be adequately informed whenever personal data is processed.

[57] The Standard Data Protection Model (v.1.0 9-10 November 2016) 27-30 <https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.pdf> accessed 12 May 2018.
[58] Ibid, 25-26.
[59] See Michael Colesky, Jaap-Henk Hoepman and Christiaan Hillen, 'A Critical Analysis of Privacy Design Strategies' (2016) IEEE Symposium on Security and Privacy Workshop <http://ieeexplore.ieee.org/document/7527750/> accessed 23 May 2018.
[60] ENISA (n 22).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

6. CONTROL: requires that data subjects should be provided agency over the processing of their data.
7. ENFORCE: requires that a privacy policy compatible with legal requirements should be in place and should be enforced.
8. DEMONSTRATE: requires a data controller to be able to demonstrate compliance with the privacy policy and any applicable legal requirements.[61]

Apart from these strategies, several techniques such as authentication, attribute-based credentials, secure private communications, communications anonymity, and pseudonymity, privacy in databases, statistical disclosure control, privacy-preserving data mining, private information retrieval, privacy-preserving computations, transparency-enhancing techniques, and intervenability-enhancing techniques were explained in the document.

These strategies were further spelt out by ENISA in guidelines that are specified in the area of big data[62] and mobile applications.[63] Recently, Jaap-Henk Hoepman explained these strategies further in Privacy Design Strategies recent publication.[64] Furthermore, the European Data Protection Supervisor (EDPS) has also published a preliminary opinion on privacy by design which brings once again to spotlight the issues of the operationalisation of the concept.[65]

There is no EU-wide harmonisation in the area of the operationalisation of privacy by design. However, a current standardisation request to the European Standardisation Organisations (ESOs) by the European Commission requests the ESOs to develop European standards and European standardisation deliverables for privacy and personal data protection management in the security industry, which considers privacy by design.[66] The objectives of the mandate are to develop European standards, which shall cover the following aspects:

> i) How to address and manage privacy and personal data protection issues during the design and development and the production and service provision processes of

[61] Ibid.
[62] ENISA, Privacy by Design in Big Data, (2015) <https://www.enisa.europa.eu/publications/big-data-protection> accessed 26 May 2018.
[63] ENISA (n 23); See also ENISA, Handbook on Security of Personal Data (2018) <https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing/> accessed 26 May 2018.
[64] Jaap-Henk Hoepman, *Privacy Design Strategies (The Little Blue Book)* (2018) <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf> accessed 6 June 2018.
[65] EDPS (n 16).
[66] European Commission, Commission Implementing Decision of 20.1.2015 <http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=select_attachments.download&doc_id=1559> accessed 6 June 2018.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

security technologies and services, allowing manufacturers and service providers to develop, implement and execute a widely recognised Privacy by Design (PbD) approach in their processes; and
ii) European standardisation deliverables addressed to the manufacturers and service providers when specifying the privacy and personal data protection management processes with an explanation how to realise them, including descriptions of the necessary roles, tasks, documentation, hardware and software requirements, and templates to be used when applying the requested standard(s).[67]

Although the standards aim among other things, at translating the concept of "Privacy and personal data protection by Design" into concrete indications for manufacturers and service providers to plan, in the security technologies and services industry, a recent opinion by the EDPS suggests that this mandate has been broadened in the wake of the GDPR to encompass other business sectors.[68] Such a standard will contribute immensely to the quest for operationalisation of privacy by design.

3.2.2.1 Other Aspects of Privacy by Design

Apart from operationalising data protection principles, the GDPR also requires that the implementation of data protection by design shall be effective and protect the rights of the data subjects. Effectiveness here implies that the rights of the data subject should not be a trade-off for securing the data, rather from the design, data subjects should have the opportunity to exercise their rights.[69] Article 29 Working Party notes that functionality should be included in privacy by design approach facilitating the data subjects' rights such as the right to revoke consent, with subsequent data erasure in all servers. Thus, implementing data subjects' rights is an integral part of privacy by design.

The GDPR contains the following data subjects' rights:

1. the right to be informed;
2. the right of access;

[67] Ibid, 4.
[68] EDPS (n 16) 16; see also Alessandro Guarino and Kai Rannenberg, 'Cybersecurity, Data Protection, and Privacy Standardization in Support of EU Policy' (Brussels 13 February 2018) <ftp://ftp.cencenelec.eu/EN/News/Events/2018/Cybersecurity_ENISA_CEN_CL_ETSI_Presentations/GUARINO_RANNENBERG_CEN-CLC_JTC8.pdf> accessed 6 June 2018.
[69] Sarah Piron 'What does the GDPR 'right to erasure' mean in practice? A view from our Belgian firm' (Ius Laboris 03 April 2018) <https://www.iuslaboris.com/en-gb/resources/insights/a/what-does-gdpr-right-erasure-mean-practice-view-our-belgian-firm/>; see also Datatilsynet (n 41); Michael Veale, Reuben Binns and Jef Ausloos, 'When Data Protection by Design and Data Subject Rights Clash' *International Data Privacy Law* (2018) doi:10.1093/idpl/ipy002 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3081069> accessed 6 June 2018.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

3. the right to rectification;
4. the right to erasure;
5. the right to restrict processing;
6. the right to data portability;
7. the right to object;
8. rights in relation to automated decision making and profiling.

Operationalising these rights in any personal data processing system means that data subjects' rights must be mapped to mechanisms to facilitate their implementation included during the design of the system. This should also be reflected in the default settings of the system.

Apart from the above general rights, the GDPR also attributes specific policies for the protection of children, which must be considered in the development of any system where children's data will be processed online.[70] This will involve enabling children to exercise their rights when using the system in a way that minimises the risks to them.[71] It entails among other things, a higher level of transparency to maximise children's understanding of the privacy policy and other information by designing it in a way that makes sense to them.[72] Therefore, the system designers should assess what the most effective method for conveying the information required under Articles 13 and 14 of the GDPR to children, including a consideration of more visually based techniques such as cartoons, pictograms, Infogrames, videos, layered information notices, pop-up notices, hover-over notices, voice alerts, etc.[73] Furthermore, where it is required that parental consent needs to be obtained for children below a certain age, then, the system must be capable of facilitating this consent procedure.

Privacy by design should also consider international data transfers, in order to implement all the necessary safeguards for such transfers as stipulated in Chapter V of the GDPR.[74] As such, all international data flows must be mapped, and legal basis for such transfers identified and before

[70] Bird & Bird, Guide to the General Data Protection Regulation - 'Children' < https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en > accessed 6 May 2018.
[71] See GDPR, recitals 38, 58, and art 12 (1).
[72] Anna Morgan, 'The Transparency Challenge: Making children aware of their data protection rights and the risks online' *The Journal of Computer, Media and Telecommunications Law (*Volume 23 No.1 2018) 44-48 <https://www.dataprotection.ie/documents/Transparency.pdf> accessed 6 June 2018.
[73] Ibid.
[74] Bird & Bird (n 70).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

the transfer. This will facilitate implementing the safeguards contemplated in the GDPR, for example, using standard contractual clauses or binding corporate rules (BCRs).[75]

In sum, looking at the legal sources and descriptions of the concept of privacy by design and by default, it stands to reason to conclude that this obligation reflects the general thrust of having a robust privacy system, and should not only target the implementation of data protection principle, but also the enforcement of the rights of the data subject, as well as facilitate compliance with other possible obligations of the data controllers such as keeping record (logs) of activities performed in the system. Due to the complex nature of the modern information system, a multi-operationalisation approach may be a viable option, in the absence of a standardised procedure, as this will allow the data controller the opportunity of analysing various guidelines and templates and adapting them to the system under consideration. The GDPR, however, considers that an approved certification mechanism may be used and code of conduct may be adhered to as evidence of compliance with this principle. In the next chapter, we consider the implementation of privacy by design in the area of disaster management.

[75] European Commission, 'Data Transfer Outside the EU' <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu_en> accessed 6 June 2018.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

4.0 Reflecting privacy by design in disaster management

As earlier indicated, the nature of disaster management operations necessitates the processing of personal data. Scenarios include where an application is developed to send alerts or warning (e.g., weather alerts or updates) to subscribers or entire population of a particular location; applications that enable citizens to access the services offered by disaster management organisations (e.g, the Red Cross); systems that process data of disaster management employees and volunteers; applications for searching missing persons during disaster; systems that are used to register refugees; etc. Given this relationship, we will consider some examples of how privacy by design has been reflected in some disaster management policies below.

4.1 Examples of the PBD Requirement in Disaster Management Policies

4.1.1 The UN High Commissioner for Refugees (UNHCR)

The UN High Commissioner for Refugees (UNHCR) is established under the UN General Assembly Resolution with the function of providing international protection to refugee and assisting governments in finding solutions to such problems.[76] As such, the agency comes in contact with disaster victims and processes their data in many circumstances. The UNHCR consolidated its privacy policies in 2015 and published a Policy on the Protection of Personal Data of Persons of Concern to UNHCR.[77] In this document, the UNHCR lays down the rules and principles relating to the processing of personal data of persons of concern to UNHCR to align with the 1990 United Nations General Assembly's Guidelines for the Regulation of Computerized Personal Data Files[78] and other relevant international instruments.

[76] http://www.unhcr.org/.
[77] UNHCR, Policy on the Protection of Personal Data of Persons of Concern to UNHCR (May 2015) <http://www.refworld.org/docid/55643c1d4.html> accessed 6 May 2018.
[78] UN High Commissioner for Human Rights, Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95 of 14 December 1990 <http://www.refworld.org/pdfid/3ddcafaac.pdf> accessed 6 May 2018.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

The policy stresses that UNHCR personnel need to respect and apply the basic privacy principles when processing personal data, and provides examples of legitimate bases upon which UNHCR may process personal data such as:

(i) Consent of the data subject;

(ii) In the vital or best interests of the data subject;

(iii) To enable UNHCR to carry out its mandate;

(iv) Beyond UNHCR's mandate, to ensure the safety and security of persons of concern or other individuals.

The policy also contains rights of the data subject including rights to information, access, correction, deletion and objection. It further provides modalities on how to enforce these rights by the subjects. Regarding appropriate technical and organisational safeguards for the security of data, the policy includes "the implementation of data protection enhancing technologies and tools to enable data processors to better protect personal data ("privacy by design and by default")". These measures were not elaborated in the policy nor were privacy by design strategies explained further in the document.

The policy also highlighted the importance of conducting a data protection impact assessment when elaborating new systems, projects or policies or before entering into data transfer arrangements with implementing partners or third parties which may negatively impact personal data of persons of concern. Implementing partners of UNHCR are equally enjoined to implement the same or comparable standards and basic principles of personal data protection as contained in this Policy.

It is difficult to assess the extent to which the principle of privacy by design is integrated into the UNHCR information system as limited information could be obtained for such systems. However, the mention of the principle in the policy suggests that the agency is aware of it and will consider it in its privacy framework.

4.1.2 The International Committee of the Red Cross (ICRC)

The ICRC operates worldwide humanitarian assistance, helping people affected by conflict, disasters and other humanitarian scenarios. It is an independent and neutral organisation; its

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

mandate stems essentially from the Geneva Conventions of 1949.[79] The ICRC adopted a Data Protection Reference Framework in February 2015 and had updated the framework since then.[80] The rules elaborate the principles of data protection and the rights of the data subject to which the ICRC subscribes to and implements in its international humanitarian actions. Article 16 of the rules contains the data protection by design and by default approach of the ICRC. It states: "While designing a database and drafting procedures for collecting Personal Data, all these rules must be taken into account and incorporated to the greatest extent possible; this is known as "data protection by design and by default."[81] This concept was not elaborated further, and no details of its implementation mechanism were included. However, in a similar policy document—*International Red Cross and Red Crescent Movement Family Links Network Code of Conduct on Data Protection*—privacy by design is seen as one of the processing commitment of the organisation. Here, taking appropriate technical and organisational measures are part of the requirements of code implementing data protection by design and by default.[82]

Furthermore, both the Code and the Framework documents also refer to data protection impact assessments which must be conducted when data processing is likely to involve specific risks to the rights and freedoms of data subjects.[83] DPIA must be carried out in such cases before the processing begins, or if during emergencies, after the processing, but as soon as reasonably possible.

4.1.3 SPEAR Project Guidelines

The Spear Project was initiated in by a group of humanitarian non-governmental organisations (NGOs) and the International Red Cross and Red Crescent Movement with the aim of improving the quality of their actions during disaster response and to be held accountable for them.[84] The project has developed a handbook containing a Humanitarian Charter and Minimum Standards in Humanitarian Response. Among the principles contained in these documents is that of protection of the rights of the victims including their privacy rights. The handbook is currently undergoing a

[79] <https://www.icrc.org/en/who-we-are> accessed 6 May 2018.
[80] ICRC, *ICRC Rules on Personal Data Protection* (2016) <https://shop.icrc.org/icrc-rules-on-personal-data-protection.html?___store=default> accessed 6 May 2018.
[81] See *ICRC Rules on Personal Data Protection*, art 16 (1).
[82] See Code of Conduct, clause 2.3.3.
[83] See Data Protection Reference Framework, art 17 and the Code of Conduct, clause 2.3.4.
[84] <http://www.spherehandbook.org/> accessed 6 May 2018.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

review, and a 2nd draft of the handbook shows that privacy and data protection is an integral part of the Protection Principle 1.[85] However, the handbook seems not to have paid particular attention to the issue of privacy by design.

4.1.4 CARISMAND Partners' Survey

A short survey was conducted among the CARISMAND partners that are involved in various forms of disaster management to understand how disaster managers operationalise privacy by design, especially in preparation for the GDPR. Five partners responded to the questionnaire. Four of the partners work directly as disaster managers, while one is only engaged in making data available for disaster response. Their responses indicate that majority of them are aware of the principle of privacy by design and its implication under the GDPR. Only one respondent is not aware of the principle but checks its system with another governmental institution for compliance purposes. All five respondents acknowledge they process personal data using a technology-based system. One respondent additionally processes personal data in a paper-based system. All respondents have internal rules on operational and technical measures to safeguard personal data as well as special categories of data.

The responses suggest that privacy by design principle is known to a large extent by the disaster managers and implementation mechanisms exist at various levels to ensure privacy, although such mechanisms may not have been tag privacy by design. However, there is also a gap in the holistic approach required under the GDPR for privacy by design, suggesting that disaster managers need to review their systems and policies in line with the new regime.

[85] The Sphere Project, 'Revising the Sphere standards' <http://www.sphereproject.org/handbook/revision-sphere-handbook/>.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

5.0 Recommendations on Privacy-Friendly Disaster Management

Work Package 6 has produced three previous deliverables on citizens' right in a disaster situation, focusing particularly on the rights to privacy and data protection, as well as cultural rights. Although the present deliverable focuses on privacy by design, the recommendations in this report build on the output of the previous Deliverables D6.1 - Report on European fundamental rights in disaster situations, D6.2 - Report on fundamental rights in disaster situations in selected national legislations and D6.3 - Report on cultural issues as provided for within select European states and their relevance in disaster situations.

The following recommendations are divided into two parts – non-technical and technical aspects and will cover issues beyond privacy by design and by default. The non-technical aspects cover the non-functionals aspects such as human rights, organisational measures, etc., while the technical aspects cover technical standards and infrastructure for data protection and security. The main audience targeted by these recommendations are the disaster managers and policymakers.

5.1 Non-technical Recommendations

1. **Adopt an overarching rights-based approach in disaster policies and operations**

   Policymakers and disaster managers should adopt a rights-based approach in their disaster policies and operations. Such an approach requires not only a proactive assessment of the human rights impact of any policy and operation in this area, but also putting in place mechanisms to enforce and realise these rights in such difficult situations. Thus, incident response mechanism to tackle cases of human rights violation is necessary in disaster management.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

2. **Support and promote research and development in the area of privacy-friendly tools used in disaster management**

   Policymakers should support and promote research and development of privacy-friendly software and systems used for disaster management. This is important to keep up with the innovation that is occurring in the use of ICT in disaster management, while at the same time promoting human rights in this area.

3. **Develop and publish guidelines on privacy and data protection in disaster and other emergency management**

   On the EU-level or Council of Europe (CoE)-level, guidelines should be published by responsible authorities such as the European Data Protection Board on the scope and application of data protection in disaster and other emergency management. Such guidelines will bring clarity and certainty to these situations and could be supplemented by clear instructions and procedures by the local disaster managers in the field.

4. **Establish coherent and transparent privacy and data protection policy**

   Disaster managers should ensure that adequate information and notices are provided to the data subjects concerning the processing of their data. These should include information on their rights and a channel for compliant and enforcement, purposes of data processing, etc. Policy on the use of social media as a source and disseminator of information is also necessary in this regard.

5. **Define specific rules on how to operationalise and achieve data protection by design and by default**

   Policymakers and other stakeholder assisted by researchers and privacy experts should engage in defining specific rules on how to operationalise and achieve data protection by design and by default in the domain of disaster management systems. The work of the European Standardisation Organisations, as well as ENISA and the EDPS in privacy by design, could form the basis for the specific application in the area of disaster management.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

6. **Carry out a data protection impact assessment before initiating a new data processing system or operations**

   Before initiating a new data processing system or procedure, disaster managers should always conduct a DPIA. Regular DPIA and privacy audit should be integrated as part of the privacy policy of the disaster management organisation.

7. **Incorporate regular training programme on privacy, data protection and data security as part of the management**

   Disaster management personnel and volunteers should constantly undergo training on privacy, data protection and data security to ensure that they are aware of the risk of privacy breach. Such training should be mandatory to ensure that all personnel understand both the need for and the risks associated with data protection and security.

8. **Anticipate innovative technology and leverage its potential for data protection**

   Disaster managers should anticipate innovative technologies for humanitarian and disaster responses and prepare to take advantage of these technologies regarding privacy protection where possible, for example, using blockchain in disaster information management. Innovative software solutions should be encouraged and sufficiently tested before they are adopted.

9. **Further research on instruments and practices relating to cultural rights in disaster management, develop operational guidelines and practice directives, and integrate modules on cultural competencies for training purposes**

   Disaster managers should carry out further research on instruments and practices relating to cultural rights within their jurisdiction and create operational guidelines to direct their activities. Such approach will assist them in cultural impact assessment, and to develop a checklist of cultural considerations relevant to their operations. They should also develop and integrate modules on cultural competencies into their existing national training programmes at all levels where none exists. The EU Civil Protection Mechanism introductory course on cultural competencies could be adapted to suit local circumstances.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

10. **Foster a proactive strategy of consultation with cultural stakeholders or communities and engage in citizen awareness**

    Disaster managers should develop proactive plans and strategies for consultation with the local and cultural communities and stakeholders during the planning and execution of disaster management activities that may have cultural impact. Citizen awareness campaigns should also be fostered, as this will facilitate a deeper understanding of the communities in disaster awareness, disaster risk perception and mitigation, volunteering, etc.

5.2 Technical Recommendations

11. **Develop a common infrastructure, based on state of the art IT-Security principles for use in disaster management**

    Policymakers should consider developing and funding a common infrastructure that conforms to privacy by design and by default principle, including IT-security for use in disaster management. This will provide disaster managers with a functional infrastructure and at the same time adequately ensure that the privacy rights of those concerned are taken care of.

12. **Implement relevant standards, code of conducts or certification relating to information system management to enhance privacy and data protection**

    Disaster managers should ensure that technologies they deploy for their operations comply with the state of the art standards and certifications and should follow best practices and recommendations from recognised institutions such as ENISA and National Institute of Standards and Technology (NIST), etc., in technical matters. All third-party functions, APIs, libraries and modules must be analysed to identify unsafe modules and functions, based on current threat levels.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

13. **Develop and provide own technical solutions for an effective and privacy-friendly disaster management and host information systems in a secure environment**

    Where possible, disaster managers should develop and provide their own technologies instead of third-party providers, as this will assist them when designing their technologies to ensure that they meet their needs, while adequately recognising and protecting human rights. Where external solutions are used, they should emphasise and encourage less privacy intrusive solutions, use only information systems such as portals or mobile applications that are hosted in a secure environment (e.g, applying end-to-end encryption and state of the art IT-security measures, etc). This will potentially secure the data and protect the privacy of the individuals whose data is processed in such systems.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

6.0 Conclusion

The principle of privacy by design and by default has been ingrained into European Data Protection Law and offers a potential tool for privacy risk management. This principle is capable of absorbing multiple approaches in its implementation once the overarching intent is to promote and facilitate privacy of the data subjects. As could be deduced from the discussions in this report, various strategies and suggestions have been put forward on how to operationalise privacy by design in general. These solutions could be adopted as complementary; it is then left for the system designers to carry out an impact assessment of their proposed operations and build-in privacy safeguards as it suits their operations. The bottle line is that conscious efforts are made at the earlier possible time of the design of the systems to incorporate privacy considerations.

For disaster managers, it is important that they understand the nature of personal data processing that is carried out in their systems. Such knowledge will assist them in implementing appropriate technical and organisational measures to safeguard such data, as well as continuously review the mechanism they put in place. This is at the heart of any privacy by design approach. Policymakers must also consider the human rights impact of their decisions relating to disaster management and should encourage a human rights-based approach in such policy areas.

The recommendations suggested above, if properly considered and implemented, would go a long way in protecting and promoting citizens' rights at the time they are most needed in difficult situations.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

Bibliography

Books, Articles, and Commentaries

AET, 'Security by Design and Secure by Default' (10 May 2017).

Behringer M, 'End-to-End Security' *The Internet Protocol Journal,* Vol 12, No.3.

Bolger P and Kelly J, 'Privacy by Design' (Lexology, 18 September 2017).

Bird & Bird, Guide to the General Data Protection Regulation - 'Children' (2017).

Bygrave L, 'Hardwiring Privacy' University of Oslo Faculty of Law Research Paper No. 2017-02.

Bygrave L, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements', Oslo Law Review, Vol. 4 No.2, 2017.

Cavoukian A, *Privacy by Design… Take the Challenge* (Ontario 2009).

Cavoukian A, 'Privacy by Design: The 7 Foundational Principles' (2009, revised 2011).

Cavoukian A, Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices (Ontario 2012).

Colesky M, Hoepman J and Hillen C, 'A Critical Analysis of Privacy Design Strategies' (2016) IEEE Symposium on Security and Privacy Workshop.

Datatilsynet, 'Guide: Software development with Data Protection by Design and by Default' (2017).

ENISA, Privacy and Data Protection by Design – from policy to engineering (ENISA 2014).

ENISA, Privacy and Data Protection in Mobile Applications (ENISA 2017).

ENISA, Privacy by Design in Big Data, (ENISA 2015).

ENISA, Handbook on Security of Personal Data (ENISA 2018).

European Data Protection Supervisor, Opinion 5/2018 Preliminary Opinion on privacy by design, (31 May 2018).

Guarino A and Rannenberg K, 'Cybersecurity, Data Protection, and Privacy Standardization in Support of EU Policy' (Brussels 13 February 2018).

Hoepman J, Privacy Design Strategies (The Little Blue Book) (2018).

Irish Computer Society, 'What is Privacy by Design & Default? (https://www.ics.ie/news/what-is-privacy-by-design-a-default).

Information Commissioners Office, 'Guide to Data Protection' (2017).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

Klitou D, 'A Solution, But Not a Panacea for Defending Privacy: The Challenges, Criticism and Limitations of Privacy by Design' in Bart Preneel and Demosthenes Ikonomou (eds), *Privacy Technologies and Policy: First Annual Privacy Forum*, *APF 2012* (Springer Verlag 2014).

Morgan A, 'The Transparency Challenge: Making children aware of their data protection rights and the risks online' *The Journal of Computer, Media and Telecommunications Law (*Volume 23 No.1 2018).

Piron S, 'What does the GDPR 'right to erasure' mean in practice? A view from our Belgian firm' (Ius Laboris 03 April 2018).

Reidenberg J et al., Privacy and Missing Persons after Natural Disasters (Center on Law and Information Policy at Fordham Law School and Woodrow Wilson International Center for Scholars 2013).

Unabhängies Landeszentrum für den Datenschutz, The Standard Data Protection Model (v.1.0, November 2016).

Laws, Regulations, Policies and Guidelines

Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679, WP 260.

Article 29 Working Party 'Guidelines on Data Protection Impact Assessment (DPIA)' Wp248rev.01.

Article 29 Working Party Opinion 03/2013 on Purpose Limitation, 00569/13/EN WP 203.

Australian Law Reform Commission, 'Regulating Privacy' *Australian Privacy Law and Practice* (ALRC Report 108, 2008); ISO 29100:2011 defines privacy principles as set of shared values governing the privacy protection of personally identifiable information (PII) when processed in information and communication technology systems.

Commission Staff Working Paper Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) SEC(2012) 72 final.

Commission Recommendation of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems (2014/724/EU).

Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive).

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as amended.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

European Commission, 'Data Transfer Outside the EU'.

HM Government, Data Protection and Sharing – Guidance for Emergency Planners and Responders (HM Government 2007).

International Conference of the Red Cross, ICRC Rules on Personal Data Protection (2016).

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 – GDPR).

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

The Sphere Project, 'Revising the Sphere standards' (2nd Ed, 018).

UNHCR, Policy on the Protection of Personal Data of Persons of Concern to UNHCR (May 2015).

UN High Commissioner for Human Rights, Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95 of 14 December 1990.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

Annex 1

Dear Partners,

Work Package 6 is conducting a final survey aimed at evaluating existing privacy by design and privacy by default approaches in disaster management frameworks. The outcome will be a set of legal and technical recommendations on how to strengthen citizens' privacy and personal data protection rights in the daily routines of disaster managers without putting the efficiency of disaster management mechanisms at risk.

We kindly ask you to complete the following questions, reflecting how your organisation has tackled or implemented privacy by design in its disaster management system.

Please send back your responses to:
nwankwo@iri.uni-hannover.de and wendt@iri.uni-hannover.de

Thank you in anticipation of your cooperation.

Privacy by Design Approach

1. Do your disaster management operations involve the processing of personal data[86] of the following:
   a) Disaster management officials and volunteers
   b) Disaster victims and their families, and/or
   c) Public

2. What information processing systems are used for processing this personal data?
   a) Paper-based system,
   b) Technologically-based system and/or

[86] According to Article 4 GDPR, 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.

c) Others, please specify

3. Is your organisation familiar with the concept of privacy by design and by default[87], and have they been considered in designing and implementing your data processing system?

4. Does your organisation has dedicated internal rules on the operational and technical measures that are applied to safeguard the personal data processed?

5. Does your organisation has dedicated rules and procedures for the processing of special categories of data[88]?

6. Does your organisation plan to reevaluate its data processing system to implement the data protection by design and by default (DbDD) requirement given the imminent effect of the General Data Protection Regulation?[89]

7. Has a Data Protection Impact Assessment (DPIA) been carried out to identify and mitigate privacy and data protection risks?

8. If a DPIA has been conducted, what mechanisms have been used to operationalize the data protection principles, rights of the data subjects, and other protection measures?

9. Does your organisation have a training programme for staff on privacy, data protection and data security compliance?

10. Does your organisation have a review and audit mechanism for data protection impact assessment, data security, and data retention policies?

[87] Privacy by Design and by Default is often interchangeably referred to as Data Protection by Design and by Default. It is a concept that encourages the design and development a system or device (i.e. software and/or hardware) in a way that supports and materializes privacy principles, values and rules as goals and functions, whereby that system or device then becomes 'privacy-aware' or 'privacy-friendly'. Privacy by default would mean that the system is preconfigured to the most privacy-friendly settings.
[88] See Article 9 GDPR.
[89] See Article 25 GDPR.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653748.