RESPECT4U – Privacy as Innovation Opportunity

Marc van Lieshout(✉) and Sophie Emmert

TNO, Anna van Buerenplein 1, 2595 DA The Hague, The Netherlands
marc.vanlieshout@tno.nl

Abstract. The right to privacy is enshrined in the European charter of fundamental rights. The right to data protection is a relatively novel right, also enshrined in the same European charter. While these rights seem to focus on a defensive and protective approach, they also give rise to a positive and constructive interpretation. The GDPR may act as driver for innovation. Not only for assuring a better way of dealing with personal data, but including a more encompassing approach of assuring privacy. RESPECT4U offers a framework of seven privacy principles that help organisations in promoting this positive attitude towards the reconciliation of privacy and innovation: Responsible processing, Empowering data subjects, Secure data handling, Pro-active risk management, Ethical awareness, Cost-benefit assessment, Transparent data processing. This paper introduces the background of RESPECT4U, and elaborates the seven principles that form its foundation. Together they demonstrate that privacy can act as innovation driver.

Keywords: Privacy · Data protection · Innovation
Privacy as innovation driver · Privacy principles · GDPR
Responsible data processing · Empowerment · Transparency

1 Introduction

The General Data Protection Regulation (GDPR) has led to heightened attention for how organisations process personal data. A relevant driver of this attention stems from the relatively high fines that organisations face when they are not compliant. These fines have parachuted the concern for an appropriate processing of personal data to the Boards of organisations. No single middle-manager can bear responsibility for fines with an order of magnitude of 2 till 4% of annual turnover. In the slipstream of these high fines the concern for data breaches and the negative impact of these breaches on the reputation of an organization adds to the growing awareness for 'doing the things right'. The GDPR also leads to controllers pushing the responsibility for a compliant processing backward to the processors they are working with.[1] Controllers are obliged

[1] See the blog post of Daniel Solove on this issue: https://teachprivacy.com/the-hidden-force-that-will-drive-gdpr-compliance/; last accessed 2018/04/08.

© Springer Nature Switzerland AG 2018
M. Medina et al. (Eds.): APF 2018, LNCS 11079, pp. 43–60, 2018.
https://doi.org/10.1007/978-3-030-02547-2_3

to work only with processors that meet GPPR-requirements.[2] Uncertainty on how the GDPR will be supervised, how data protection authorities will fill in their role, and how the many open issues within the GDPR need to be understood, feeds criticism on the GDPR as being an instrument that might negatively impact business opportunities in today's data driven economy (London Economics 2017). Losses could amount up to 58 billion UK pounds for the whole of the EU (UK still included). These losses come among others from organisations moving data analytics back to in house processing instead of hiring third party capacity with specific expertise and competences in doing the analytics. So, innovation might be stifled by these organizational responses.

When these negative implications would largely determine the impact of the GDPR in the long run, one might wonder whether the GDPR could play a role in promoting the free flow of data within the EU and in being an instrument in the Single Market Strategy of the European Commission. This is an interesting dispute by itself. Long term economic perspectives of the strategy chosen are based upon presumptions of how market players will react. One reaction one can already observe is an increasing awareness by these market players for the additional requirements posed by the GDPR. Staying in business within Europe means meeting these requirements. The two-staged strategy that is adopted by some big players (such as Google and Facebook) means that they are both looking for alternatives outside the influence of the GDPR while not alienating themselves fully from the European scene.[3]

Whether this approach will be profitable for European citizens ánd for the European economy in the long run is hard to predict yet. At least we can notice the emergence of a consultancy market that focuses on providing advice and supporting organisations in becoming compliant.[4] This by itself is a positive side-effect of the GDPR.

In this paper we would like to argue that the rigid and encompassing implementation of the GDPR has a beneficial impact on the innovative capacity of organisations and will lead to new innovative services. Our approach is conceptual yet. We are not able to provide empirical evidence for our assumptions in this stage. We only are able to develop a 'line of reasoning' that clarifies our position with respect to the potentially beneficial role of privacy as a driver for innovation. Recent events that highlight the detrimental implications of surreptitious use of personal data for political purposes

[2] GDPR, art 24(1): "… the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.", Art 28 (1) "… the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."

[3] See for instance https://www.privacylaws.com/Publications/enews/International-E-news/Dates/2018/4/Facebook-shifts-15-billion-users-to-avoid-GDPR/ and https://martech-today.com/facebook-well-implement-gdpr-privacy-protections-globally-213545, showing both sides of the coin. Last accessed 2018/05/20.

[4] See for instance https://gdprindex.com/, a website that provides an overview of firms active in providing consultancy services of various kinds.

demonstrate that the overall societal attitude towards these kind of practices is changing and may promote more responsible organisational behaviour.[5]

This paper starts by outlining the distinction between privacy and data protection and will outline how the two concepts can be reconciled in an approach to promote innovation. Then, RESPECT4U is introduced and elaborated. Basically, RESPECT4U captures seven privacy principles that together create a framework to support organisations in combining 'doing the things right' with 'doing the right things'.

2 Privacy and Data Protection: Two Sides of the Same Coin

2.1 Privacy as a Concept

It is a challenge to succinctly define privacy. Many authors have claimed that such a succinct definition simply cannot be provided, given the differences between countries, cultures and civilisations in how issues such as what is considered to be public and what private are evaluated, what role property plays and how politics is organised. One line of reasoning refers back to ancient civilisations, such as the Greek one in which being public meant being able to act as a person (Van der Sloot 2017). The etymological source of the word 'person', from 'per sonare', basically stipulates the ability to be heard. It refers to the habit of actors in the theatres wearing a mask that enabled amplifying the voice. Opposite the public arena we find the private household, the domain of wives and slaves. The root of the word 'private' is the word 'privare', meaning being robbed of something.[6] It was important to be able to act as a public person in ancient times. While the household was shielded off public appearance, this was mainly because of the non-relevance of the household, and not because of respect. In a similar vein were slaves property of their owner. In present times, we consider the home and the body to be sacrosanct (though admittedly, this is not always enacted). We find references to the privacy of the home in the eighteenth century, through the following statement of the English statesman William Pitt the Elderly:

"The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail, its roof may shake; the wind may blow through it; the storms may enter; the rain may enter – but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement".[7] (Holvast 1986, 11–12)

---

[5] The 'Cambridge Analytica' casus is a clear point in respect. This organisation has acted quite irresponsibly in its strive to influence people's behaviour by illegitimately using knowledge on their postings on social media. While one could question whether 'nudging people' is unethical by itself, the unlawful processing of personal data by Cambridge Analytica is a clear infringement of legal obligations in offering choice and consent to people.

[6] The second meaning given in the dictionary is to liberate. The meaning of 'being robbed' is however also present in the Spanish meaning of the word 'privar'.

[7] The statement was made during a debate in the House of Parliament in 1773 where it was discussed whether the Crown's forces were entitled to search in houses for evidence of the production of cider in order to levy taxes. See https://www.chroniclesmaga-zine.org/blogs/thomas-fleming/defending-the-family-castle-part-i/; last accessed 2018/04/08.

The very physical dimensions of privacy (the home and the body) are complemented by non-physical dimensions. This has two faces: privacy with respect to relations and privacy with respect to information.[8] The last one is a typical dimension that increasingly becomes relevant in modern societies. Large parts of current behaviour is intermediated by digital technologies. Controlling access to these technologies and especially controlling access to one's behaviour that becomes manifest through these digital technologies is a 'natural' extension of this notion of privacy. The emerging lack of control on who should have access to one's behaviour formed the starting point for US based lawyers Samuel Warren and Louis Brandeis to write their seminal paper on the right to be let alone (Warren and Brandeis 1890). Samuel Warren was married to a senator's daughter and his wife was portrayed in a tabloid without her knowing it. In these days, it became possible to photograph a person without that person's consent, due to creating camera's that were lighter and mobile and especially faster in producing the photo. This invasion of privacy was condemned in the article. Their article is still worth reading, for instance for the manner in which technological progress and its impact on society is tackled.

Attention for privacy, or the right to respect for a private life, became one of the focal points in the 1948 Universal Declaration of Human Rights in the aftermath of the Second World War. The Declaration was an attempt to organize universally accepted ethical standards that should help preventing the experienced atrocities of the Second World War, including its devastating infringements upon human rights.

The European Charter of Fundamental Rights, enacted in 2009 through the Lisboan Treaty, reiterates this right to respect for privacy. The Universal Declaration of Human Rights states in article 12: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation." The European Charter of Human Rights formulates in Article 7 that "[e]veryone shall have the right to respect for his or her private life, family life, the home and communications".

While Declaration and Charter coincide in embracing the broader concept of privacy, the European Charter is the first declaration that pays explicit attention to the respect to data protection. Article 8 of the Charter defines a right to the protection of personal data. These data must be processed "fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."

2.2 The Concept of Data Protection

Article 8 of the European Charter for Fundamental Rights characterises a relevant development in dealing with personal data. While the emergence of data processing equipment was only in its infancy shortly after the Second World War, and no direct

[8] See (Finn et al. 2013) for an elaboration of seven dimensions of privacy including the right to relational privacy. In this paper we will stick to the four privacy dimensions that are commonly recognized as relevant ones: information privacy, relational privacy, spatial privacy and bodily privacy.

connection between the protection of privacy and the protection of personal data can be inferred from the acceptance of the Universal Declaration of Human Rights, the scenery changed considerably in the decades to come. This heightened attention for the impact of data processing on the respect to the privacy of citizens led to the USA Privacy Act in 1974. This Privacy Act was the direct consequence of a 1973 report of the Department of Health, Education and Welfare on the rights of citizens concerning records made on them.[9] The report recommended that no database should be kept in secret, that individuals should be informed about processing their data in databases, and that a so-called Code of Fair Information Practices should be established. This Code should detail issues such as purpose specification, right to be notified, right to access, right to rectify and the obligation of the processor to assure the quality of the data processed. The OECD adopted the approach of the HEW and the US Privacy Act and initiated the Fair Information Principles in 1980 (updated in 2013, keeping the original principles intact) (OECD 1980). In 1981, the Council of Europe followed suit with Convention 108, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (Council of Europe 1981). The Convention used the same principles as set out in the OECD Fair Information Principles. It introduced the notion of special categories of data (article 6). Principles such as purpose specification, collection limitation, quality of data, use limitation and storage limitation are key to the Convention (article 5). Right to access, rectification, erasure and presentation of a copy of the data are present in the Convention (article 8), as well as necessary security safeguards (article 7). Being signed by five Member States of the Council of Europe would make the Convention entering into force, implying that these Member States should implement domestic laws reflecting the Convention. The Convention entered into force October 1, 1985, being signed by France, Germany, Norway, Spain and Sweden.[10] Several countries followed suit in the following years. The last signatory yet is Tunesia in 2017, turning the total number of signatories to 51 at this moment in time.

The principles set out in the OECD FIP and Convention 108 were copied into the Data Protection Directive of 1995 for the countries of the than European Community. Being a Directive, many differences in the implementation between Member States exist. This caused confusion and a distorted level playing field, for instance for business organisations that wanted to roll out business propositions over various EU countries. This has led to the harmonisation over countries within the European Economic Area (Member States of EU plus Lichtenstein, Iceland and Norway) by the General Data Protection Regulation (2016/679/EU).

[9] See https://epic.org/privacy/hew1973report/ for a web-based version of the report. Last accessed 2018/04/08.

[10] See https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures; last accessed 2018/04/08.

2.3 Innovation Privacy and Data Protection

The previous sections have presented concise overviews of privacy and data protection as concepts. Both deal with the protection of persons, with safeguarding fundamental rights persons may exercise. While infringement of the right to privacy means that some substantive right is infringed (such as the violation of the body, the home, the reputation of a person), an infringement of the right to data protection means that a procedural right is infringed (such as the right to assurance of the quality of the data processed, or the right to be informed about the data processing) (Gellert and Gutwirth 2013). The distinction between the two types of infringements is visible in the Courts dealing with the infringement: in case of privacy one ends up at the Court of Human Rights in Strassbourg, while in case of data protection one ends up at the Court of Justice in Luxembourg.

The procedural rights as formulated in the GDPR are meant to assure the substantive rights to privacy as laid down in the European Charter (and in constitutional laws of European Member States). These rights thus serve an end in themselves but serve another end as well.

Returning to the objective of this paper, the issue to be tackled is thus whether the GDPR in promoting privacy enables or even enforces innovation or whether it hinders or blocks innovation. The rise in organisations offering compliance tools and services indicates that the economic impact of the GDPR is more than the study of London Economics seems to hint at (London Economics 2017). For sure, the GDPR limits specific forms of data processing that at present are at the heart of the business processes of data brokers and data intensive organisations of any kind (financial services, public services, traffic and transport, energy, health care, etc.). The services offered by these organisations may be at odds with the GDPR while they represent business opportunities. But being at odds with the GDPR implies that these business opportunities may confront human rights and may have adverse societal and individual consequences. The challenge to be addressed is the balance between economic growth perspectives for business organisations involved, interesting new services at the expense of potentially societal implications such as discrimination, exclusion and stigmatisation, and societal justice. While we have experienced the rise of practices that emphasize the first part of the balance (economic growth) we now observe the pendulum swinging back to include the other part of the balance as well. We signal a similarity with the (societal) debate that started in the sixties of the past century and that by now has led to heightened attention for including sustainability objectives in industrial and service practices, leading to organisations profiling themselves as being sustainable and green.[11]

The question to be posed is whether the GDPR promotes specific innovative practices and if so, how these could be organised. We have developed a framework, RESPECT4U, that demonstrates how these innovative practices might be identified from a GDPR perspective. We will now turn to this framework.

[11] This similarity may be larger than it seems to be at first glance. The GDPR may have a similar impact on business processes: from resistance to embracement and inclusion in the very heart of business activities.

3 RESPECT4U as Innovation Framework

In our work as privacy researchers of a Research and Technology Organisation we see many organisations struggling with the implementation of the GDPR. The requirements the GDPR imposes on organisations are not be underestimated. While this heightened attention for how to responsibly process personal data for sure has a positive impact for the privacy of the data subjects it easily leads to administratively 'ticking the boxes' as a way of coming to terms with the GDPR. This is enforced by uncertainty about how the Data Protection Authorities (DPAs) will fill in their role. While the GDPR explicitly demands the DPAs to be advisory and supportive, next to tracking the 'bad guys', the fines DPAs may enforce easily tips the balance for organisations to remaining on the safe, administrative, side.

This focus on fulfilling legal obligations without additional benefits for organisations may be a dead end in itself. No positive stimulus, no reward, seems to be baked into the legislative approach. On the other hand one can notice a positive undertone in quite a few contributions on the role the GDPR might play in organisational processes concerning how to deal with the data of their customers, clients, patients, students, etc.[12] And this positive tone is not only uttered by 'usual suspects', such as the International Association of Privacy Professionals[13], but by advertisement organisations such as Experian as well.[14] The basic assumption is that the GDPR may have a positive impact upon trust of consumers on how organisations will handle their data. Since the GDPR requires all organisations to implement specific requirements, simply fulfilling these requirements will not easily serve as a Unique Selling Point for organisations. Of course, frontrunners can do so and can offer this as a feature to differentiate themselves at the market place. But in the end, all organisations need to comply. Our position is that it is not so much compliance that is at stake but the manner in which organisations adopt a comprehensive perspective vis-à-vis the role of processing personal data in their business processes, and the manner in which they embed this, communicate it and innovate their services and products taking responsible processing as a starting point. And this is precisely where RESPECT4U enters the scene.

3.1 The Privacy Principles of RESPECT4U

RESPECT4U is an acronym referring to seven privacy principles:

- *Responsible* processing of personal data
- *Empowering* data subjects
- *Secure* data handling
- *Pro-active* engagement of data processes

---

[12] See for instance https://www.computerweekly.com/opinion/Why-Europes-GDPR-privacy-regulation-is-good-for-business; https://www.computerweekly.com/news/252435774/GDPR will-have-positive-ripple-effect-say-US-consumer-group. Last accessed 2018/04/14.

[13] https://iapp.org/news/a/why-the-gdpr-is-good-for-businesses/. Last accessed 2018/04/14.

[14] https://www.edq.com/uk/blog/8-reasons-why-the-gdpr-can-help-boost-your-business/; last accessed 2018/04/14.

- *Ethical awareness* on (long term) implications
- *Cost and benefit assessment* of responsible data processing
- *Transparency* re. internal organisation and data subject.

The addition '4U' has a specific meaning. It refers to 'U', being the data subject, '2U', being the data subject in relation to another person, '3U', representing 'three is a crowd', and '4U', referring to the crowd of crowds or society at large. RESPECT4U indicates that privacy is not only an individual concern but has its footing in democratic society itself and should also be evaluated on its impact on democracy as a political system (Bennet and Raab 2006).

The seven principles of RESPECT4U capture the obligations of data controllers and processors and meet the rights of data subjects as these are laid down in the GDPR. But it does not stop there. It also asks attention for new challenges ahead, such as those emerging from new data analytics and use of sophisticated machine learning techniques. And it also asks to look at the value perspective of privacy, both from an ethical position and from a more mundane position, looking at costs and benefits.[15] While the acronym presents the various principles in a specific order this is just an artefact of using an acronym that enables an easy manner of organising activities and instruments. It does not include a value judgement regarding the relevance of the principles. Still, the whole process starts with the need to responsibly process personal data. This being followed by attention for empowering data subjects puts emphasis on the relevance of involving data subjects, but that is just coincidentally second. Together, the seven RESPECT4U privacy principles help promoting innovative behaviour of organisations by 'doing the right thing' (safeguarding privacy) in the right manner (data protection). We will now introduce the various principles.

Responsible Processing

The first principle is the principle that organisations are determined to act responsibly with the personal data they process. The current data society has turned (personal) data into the fuel of many business activities.[16] The data ecosystem that has emerged and that embeds data brokers, data analytics organisations, data scrapers, etc., has become extremely complex over the past few years (Stone 2014). There is no need to be naive about the economic value of personal data, the business processes that are yet in place to capitalize on these data and the potentially adverse implications that this may have on the privacy of individuals.[17] But this does not mean that it is a complete lost case. As indicated above, the past has demonstrated that public awareness may have a

[15] Costs and benefits do not only relate to financial or monetary aspects, as we will demonstrate further on.

[16] This refers to the famous saying that data is the new oil. Quoted by many, the origin of the quote is not fully known. See https://www.quora.com/Who-should-get-credit-for-the-quotedata-is-the-new-oil. Last accessed 2018/04/14.

[17] The recent uproar concerning the activities of Cambridge Analytica and the role Facebook played is a point in respect.

decisive influence on business activities and business behaviour.[18] The basic principle thus is that organisations are actively willing to promote responsible processing of personal data, and are willing to demonstrate this responsibility.

The GDPR offers a number of instruments that organisations can use for demonstrating accountability. Code of conducts and certification mechanism are novel instruments. The manner in which certification mechanisms will enter the market place, is an open issue.[19] They may play a role in standardizing requirements and ways of working. Certification organisations, such as EuroPriSe[20], are already active on the market and offer GDPR compliant certification procedures. Issues that need to be resolved are the transferability of certificates between countries, and the role DPAs will play as accrediting organisation, next to national accreditation organisation. The same goes for codes of conduct. Various branches are already active in creating branch-oriented code of conducts that in due time will have to be approved by national DPAs. Branch-wide subscribed codes of conduct may promote a positive image among clients and customers.

Another instrument to be used is the Privacy Maturity Model. The Dutch Centre for Information Security and Privacy Protection (CIP) has used the PMM to develop a guideline that helps organisations in scoring how privacy mature they already are.[21] This uses the well-known gradation from ad hoc up to fully organised.[22] The model can be used to score progress on the implementation of the GDPR. Consultancy organisations are developing their own schemes to be put on the market, and add options for fulfilling the GDPR obligations. These are valuable instruments, as long as they are combined with additional instruments.

They may be accompanied by an internal Data Protection Officer who is entitled to supervise internal processes. A DPO may supervise the legitimacy of goals and grounds of data processing within the organisation, and offer support when it comes to fulfilling obligations such as keeping a register of processing operations and performing a data protection impact assessment. The DPOs are the contact point of the organisation with the national DPA in case of issues concerning data protection, including data breaches.

---

[18] Public (and political) awareness concerning the need to change to sustainable production modes has had a decisive influence on the dominant role of becoming and being sustainable. While differences with 'data pollution' we are experiencing today are obvious, both practices share some similarities as well. See for instance the presentation of Van den Hove during a Conference on sustainability organized by EWI Vlaanderen. https://www.ewivlaanderen.be/sites/default/files/rri_sep2016_vandenhoven.pdf. Last accessed 2018/05/21.

[19] We are participating in a research project for the European Commission in which we study the manner in which art 42 and 43 of the GDPR should be understood and should be operationalized. The results of this study are not publicly available yet, as the study has not been completed. Finalization is foreseen for June 2018.

[20] See https://www.european-privacy-seal.eu/EPS-en/Home; last accessed 2018/04/16.

[21] See https://cip-overheid.nl/privacy-baseline; last accessed 2018/04/16.

[22] Initially developed for scoring the maturity of business processes in the Capability Maturity Model (Paulk 2002).

Empowering Data Subjects

The GDPR is focused on offering data subjects more control over their data. After all, the data somehow originate from their activities and behaviour. The GDPR obliges controllers and processors to organise the rights of data subjects. Instead of just indicating to data subjects that their data are safe and appropriate safeguards have been taken – as can be read in current privacy statements – while data subjects have no clue about the kind of data processed and the kind of security safeguards taken, RESPECT4U promotes a more active role by controllers.

Empowering data subjects means they get a real stance in the data processing operations. This starts by being fully informed on what data processing operations are being executed. While this is an obligation, imposed by the GDPR, it can be fulfilled in various manners. We propose to start by the information needs of data subjects and by their basic behavioural predispositions, thus including behavioural economics as a discipline that may be of help.

Concerning the first, the information needs, we build upon the work of Alan Westin, who has executed many surveys investigating privacy preferences of data subjects (Kumaraguru and Cranor 2005). Westin differentiates between three main categories of persons in respect to their privacy attitude: fundamentalists, pragmatists and unconcerned. The fundamentalists have a very critical attitude vis-à-vis organisations, pragmatists adopt a pragmatic attitude and are willing to negotiate with organisations and unconcerned have a relatively relaxed attitude vis-à-vis organisations and trust these organisations to take their interests into account. The main thing to emphasize here is not whether this model captures the intricacies of human behaviour sufficiently, but rather to open up an undifferentiated perspective on the data subject. In our research we have performed similar surveys to understand the impact of perceptions and preferences of persons (Vos *et al.* 2016; Van den Broek *et al.* 2017). This has led to the creation of a model in which we change the perspective from privacy as the determinant factor where to focus on towards 'willingness to share' as the predominant feature relevant to take into account. This model is based on insights offered by behavioural economics, presuming that the manner in which people are willing to engage in a negotiation will depend on the offer made, behavioural predispositions and the context. Several experiments show the relevance of the behavioural predispositions and contextual factors (Acquisti 2009, 2016; Jentsch *et al.* 2012). Many behavioural characteristics influence the privacy attitude (and the willingness to share) of persons. When informing data subjects these differences should be taken into account.

Secondly, next to informing people, it is relevant to determine what kind of control should be exercised by data subjects. Again, we use the differentiation between privacy preferences, attitudes and contextual factors on how to offer control. Overall, people indicate they appreciate the option to control (Vos *et al.* 2016; Van den Broek *et al.* 2017). But exercising meaningful control implies that data subjects fully understand the impact of their choices. Once more, given the complexity of the data ecosystem that has been created one cannot presume that these complexities will be understood by all. Using distinct categories of data subjects may help in the way control should be structured. From a number of experiments we performed for commercial organisations we learned that offering meaningful information and control was supportive to the willingness to share. Overall, data subjects were quite open in sharing data for public

interest issues (such as crowd management and health issues) as long as they could be sure that their data would only be used for these purposes.[23]

Security

The third privacy principle relates to secure handling of personal data. Three perspectives can be distinguished:

1. The secure storage of data
2. The secure processing of data
3. The secure access to data

The first of these issues is well understood. Encrypted storage of data is part of normal practices. ISO norms (27001) require usage of encryption keys sufficiently strong to prevent data easily be deciphered when hacked or coincidentally released.

The second and the third bullet point are more open to innovative approaches. New cryptographic approaches are under development for the secure processing of data. Homorphic encryption and multiparty computation are techniques that enable processing of encrypted data in encrypted space such that meaningful results still can be derived (Erkin *et al.* 2012; Bost *et al.* 2014; Veugen *et al.* 2015). New techniques are under development that have the algorithms transferred to the data instead of the other way around.[24] Another technique combines polymorphic encryption and pseudonymization (Verheul and Jacobs 2017). While a number of these techniques are embedded in pilot projects, they are not sufficiently mature to be presented as a commercial product. One such product, the IRMA technology, has created its own foundation seeking for interested commercial parties to explore the potential of this novel attribution based credential system, minimizing data that are needed to identify a person in specific situations.[25] All these techniques, while partly still in their infancy, will help organisations to create more secure data processing systems that not only are more secure than current ones but that also directly help in promoting privacy respecting practices.

Pro-active Attitude

The fourth privacy principle relates to the newly introduced principles in the GDPR concerning the data protection impact assessment (DPIA), and data protection by default and design. These principles underscore the risk approach of the GDPR. Identification of risks and presentation of mitigating measures to reduce the risks such that they become manageable (or the risk residue is considered to be acceptable) are crucial elements for controllers in coming to terms with their legal obligations. While several instruments are on the market, helping organizations to perform a data protection impact assessment, the concept of data protection by design is as yet not really understood. The GDPR mentions data minimization as data protection principle and pseudonymization as instrument to achieve data protection by design. But this seems to

[23] These experiments were performed for commercial organisations. We cannot support these claims by public data yet. We hope to do so in the near future.

[24] See https://www.dtls.nl/fair-data/personal-health-train/; last accessed 2018/04/15.

[25] See https://privacybydesign.foundation/irma/; last accessed 2018/04/15.

be not more than just an initial (though relevant) step. Using pseudonymization by default in organizing the processing of personal data will definitely have a beneficial impact upon the protection of rights and freedoms of data subjects. But there are more options to be explored.

The DPIA is an instrument that is already part of standard repertoire of many organisations and national DPAs (Wright and De Hert 2012). The focus of DPIA's is on the possible infringements of data processing on the rights and freedoms of individuals. These individuals can be data subjects but they can also be persons affected by the processing without having their personal data processed. This is a consequence of profiling. Having profiles introduces the risk of being victimized by proxy, for instance because a specific profile has a geographic basis and an individual living in the specific geographic location is considered to fit to the profile. These kinds of risks need to be taken into account when performing a DPIA. One of the major challenges for identifying the level of risk is whether the risk should be seen as a high risk or as an ordinary risk. Though the GDPR adopts the basic approach of risk being a function of frequency of occurrence and level of impact, it hardly details how a high risk should be defined.[26] It is rather obvious that the engineering approach of risk, that is based upon industrial tests of components of instruments, will not work in determining the likelihood of occurrence of an infringement of rights and freedoms, let alone the determination of the impact when an infringement occurs. Within the research organisation we are working in, PhD students work on how the engineering approach of a risk can be reconciled with a legal and societal perspective.[27] This work is quite relevant given the heightened attention for risk in the GDPR, and the fact that through risk the protection of persons with respect to the processing of their data has direct links with the notion of the right to privacy and the avoidance of infringements on rights and freedoms of data subjects. Concerning data protection by design, Ann Cavoukian has pioneered in offering a set of privacy by design principles (Cavoukian 2011). This approach has meanwhile been taken a step further by privacy engineers. They have organised themselves in a network and they have started working on the elaboration of so-called privacy strategies and privacy patterns (Colesky *et al.* 2016; Danezis *et al.* 2014).[28] The work of Colesky and others focuses among others on various strategies to streamline the data process itself. This leads to four design patterns: Minimize, Separate, Abstract, and Hide. It has hooks towards data subjects (Inform and Control) and to organisations (Demonstrate and Enforce). The strategies are being translated in patterns that in the end should yield

[26] The Article 29 Working Party has produced guidelines fort his identification but these guidelines are also not decisive and leave many items open (such as the definition of 'systematic' and 'large-scale'). The GDPR indicates that a list will be developed that may contain processing operations in need of a DPIA and a list of operations not in need of a DPIA, but it may take some time before such a list has been concluded. (Art29WP 2018)

[27] Our research organization, TNO, collaborates with the Radboud University and Tilburg University in the Privacy & Identity Lab, PI.lab, on digital privacy and electronic identity issues. The PI.lab brings together researchers of various disciplinary backgrounds in order to create a multi-disciplinary approach of privacy in current day data processing. See https: www.pilab.nl; last accessed 2018/04/16.

[28] See IPEN, International Privacy Engineering Network https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_en; last accessed 2018/04/15.

viable products to be used by whoever is interested. This final steps is still under construction, though for specific patterns tools are already available.[29]

Ethical Awareness

Privacy is related to human dignity, to exercising autonomy, to mastering your own destination. The risks that will be identified in a DPIA are risks relating to the infringement of these rights and freedoms. The freedom to behave autonomously, for instance. Awareness for these infringements is growing, for a number of reasons. For one, the practice of nudging that prominently came to the fore in the Facebook-Cambridge Analytica case, might indicate a kind of landslide concerning the legitimacy of these practices.[30] The results of the empirical research into the personality features of the participants has been made public and are part of scientific literature (Youyou *et al.* 2015). It is the application of the results in specific contexts (endangering the right of persons to freely determine whom they should vote for) that led to societal uproar, leading to Congressional hearings in the USA and a public hearing in the European Parliament.[31]

These ethical concerns have been fed by the discussion on the ability to explain the logic of automated decision making. This is another issue that relates to the GDPR but has its own dimensions as well. Having machine learning techniques that are essentially non-deterministic implies that the logic of these algorithms can be explained up to some degree of understanding (such as "the weights used within the algorithm will vary with the input offered") but this does not lend any credibility to the outcome of the algorithm ("now you belong to a specific category; this may change however in the future, depending on new calculations"). This may lead to quite unsettling disputes, especially concerning outcomes that may have legal consequences or have a significant impact upon persons. The emergence of the Internet of Things with its impact upon automatic decision making by systems fed by sensor data (in automated driving, in household energy systems) will contribute to the need for ethical decision making as well (Hildebrandt 2015).

Other concerns relate to bias in data and bias in the algorithms used. Critical reviews have been published that demonstrate how biased data will reproduce the initial bias in its outcome and as such may have adverse selection consequences for groups of individuals that unluckily fall under these biases (EOP 2016). The reports also demonstrate the problem of being aware of what kind of biases might sneak into datasets.

Societal issues concerning how outcomes of data analyses may lead to ethical choices that have an impact upon the autonomy of persons are also demonstrated. One

---

[29] See the literature on for instance k-anonymity and trusted third parties that play a role in organizing these patterns. (Barker *et al.* 2009; Palmer *et al.* 2000).

[30] See e.g. https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html and https://www.washingtonpost.com/business/understanding-the-facebook-cambridge-analytica-story-quicktake/2018/04/09/; last accessed 2018/04/16.

[31] See https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.cf7c8e3ff87c and https://www.independ-ent.co.uk/news/uk/politics/mark-zuckerberg-eu-parliament-house-commons-uk-hearing-fa-cebook-data-a8361066.html; last accessed 2018/05/21.

such case relates to predictive policing. The Chicago police uses data analytics to predict gun violence. Having determined potential criminals the police pay a visit to the criminals-to-be that they will be observed in order to prevent gun violence to occur (Saunders *et al.* 2016). Another pilot has been run in the Dutch city of Eindhoven in which sensor technology was used to predict uproars in a street where youngsters came together during weekends to party. The focus was on the stifling effect these interventions may have and the ethical concerns related to these stifling effects (Galic 2016).

Finally, more 'mundane' ethical issues relate to unfair treatment, discrimination, exclusion and stigmatization as a consequence of data processing. The data processing itself may be fair but the impact may have these kinds of consequences. The complexity of present-day data ecosystems makes it more difficult to keep control over parameters that determine group profiling and consequences thereof (Van der Hoven *et al.* 2012). Coping with these ethical issues may introduce the need for ethical impact assessments and may lead to inclusion of ethical principles in designing data processing systems. This is a field of expertise that receives quite some attention in engineering disciplines, and is also known as value sensitive design (Steen and Van der Poel 2012; Van der Hoven and Manders-Huits 2009).

Costs-Benefits Assessment

Usually privacy and data protection are seen as cost factors: the organization needs to make costs for the implementation of security measures and for becoming compliant with the GDPR. Systems need to be adapted, personnel need to be trained, procedures need to be developed, implemented, maintained and supervised. Especially for small organisations, the legal expertise needed to fully understand the requirements to fulfil is not present in the organization itself, and needs to be acquired through third parties. This is costly, time consuming and when direct benefits are absent, a hurdle to overcome, in a fast-moving consumer market where new releases of products may take no longer than three months after the last one.

Balancing costs and benefits is confronted with a number of difficulties: costs can be calculated in hard coins, such as investments to be made, while benefits may be soft (increase in trust in the organization) and longer term oriented. Analyses of previous cases demonstrated that losses (in stock market value, for instance) were usually limited to a couple of days or weeks, and usually rather modest in scale (Acquisti *et al.* 2006).

Again, the Facebook/Cambridge Analytica casus may be a turning point in history, though that is at this moment in time hard to predict.[32]

Privacy is also studied in its impact on economy as a societal subsystem (Acquisti *et al.* 2016; LSE 2010). Acquisti *et al.* (2016) demonstrate that it is still pretty hard to come to conclusive arguments with respect to the economic value of privacy. The economic theory of privacy becomes more nuanced now more empirical relations have been investigated by various scholars. Apart from issues on micro-economic behaviour (see above), the existing information a-symmetry between data subjects and the

[32] The bankruptcy of Cambridge Analytica demonstrates that consequences of social condemnation may be severe. See https://www.reuters.com/article/us-cambridge-analytica-bank-ruptcy/cambridge-analytica-files-for-chapter-7-bankruptcy-idUSKCN1IJ0IS; last accessed 2018/05/21.

organisations processing their data leads to systems imperfections that have an impact on the innovative capacity of these data systems. To overcome this hurdle, increased transparency and investing in trust relations are key.[33]

Transparency

The last privacy principle relates to transparency. It connects transparency to trust, an essential ingredient of the relation between an organization and its clients. Studies have demonstrated the positive relation between information transparency and consumer purchasing attitudes (Baduri and Ha-Brookshire 2011) and on value chain partners (Eggert and Helm 2003). Information transparency is a concept that needs to be understood in terms of what information in what circumstances in what form to what participants for what purposes is enfolded (Turilli and Floridi 2009). The studies we performed demonstrate that people highly appreciate transparency as part of control options (Van den Broek *et al*. 2017). The transparency promoted by the GDPR may help in promoting trust in the processing of personal data by organisations and may thus have a positive impact upon service uptake. This relation is however not a strict linear one, in the sense that more transparency always positively impact upon trust. Trust online unfolds in a dialectic relation in which too much transparency may lead to a world that becomes too familiar and that may have negative consequences, for instance when transparency makes apparent that shared values and perspectives are absent (Keymolen 2016). Again, this indicates the relevance of connecting the data subject to the purposes and goals that are connected to the processing of personal data and to include user preferences in these goals and purposes.

Another perspective of transparency emphasizes the internal transparency within organizations. This implies that organizations include all personnel in its privacy policy and implement responsibilities, roles and rules in a transparent manner. One way to promote this is by appointing Privacy Champions within your organization and using them as the ambassadors of a privacy respecting approach.[34]

4 Conclusions

The seven privacy principles of RESPECT4U embed a perspective on organizational approaches to privacy that promotes privacy as a positive driver for innovation and for businesses. It refers to a number of instruments and tools organisations might implement in order to meet the requirements of the GDPR in a systematic and structured manner. Organisational measures, such as indicated in the Responsible and Transparency principle are complemented with technical measures such as indicated in the Security principle. Technical measures are also embedded in the Pro-active principle that promotes a comprehensive approach towards privacy by design/default. Technical measures as promoted in the Security principle can be implemented to achieve a proper

[33] See http://blogs.lse.ac.uk/mediapolicyproject/2016/07/27/the-economics-of-privacy/; last accessed 2018/04/16.

[34] See https://privasee.blog/2015/11/18/do-you-have-privacy-champions-in-your-organisation/; last accessed 2018/04/16.

realisation of privacy by design/default. The Empowerment and Transparency principle focus on understanding how consumers/citizens might be helped best in offering tools to help them exercising their rights and understanding what is done with their data. Our perspective in this respect is that it will help promoting the willingness to share data, or the willingness to remain engaged in receiving business or public offers that may be beneficial to them. In the Ethical principle we have outlined some issues that will lead to innovative practices but that also will shed light on potential show-stoppers. Cost and benefits, as last principle, will help understanding the potential business benefits of embedding privacy strategies in organisational and service oriented processes and will also demonstrate pitfalls and barriers.

All in all, the framework intends to overcome a too narrow perspective on data protection and the obligations as put forward by the GDPR. It focuses on privacy as the societal value to be respected and data protection (or, more precisely: the protection of persons with regard to the processing of their data) as the inroad to this societal value. Many of the measures proposed through any of the RESPECT4U privacy principles are oriented on fulfilling obligations of the GDPR. But in their entirety and in the combination of these principles with the measures that are aimed at furthering a better understanding of behaviour of data subjects, and understanding ethical concerns on – future – data processing activities (such as with AI), they go beyond mere compliance and offer an encompassing perspective on responsible processing of personal data, aimed at safeguarding privacy while promoting beneficial services.

The challenges to realise the real innovative potential of privacy are manifold. It requires a multi-disciplinary and multi-layered attitude. Multi-disciplinary, since it is necessary to integrate legal, technological, organizational and societal perspectives on privacy. Multi-layered since it runs from purely organizational activities to understanding behaviour and implications on a more generic level. RESPECT4U outlines an agenda that might help in coping with the various challenges in a coherent and encompassing manner. It enables the identification of practical tools and approaches that can

directly be implemented by organisations. Thirdly, it can also simply be used as a pictorial that enables discussing the 'privacy stakes' for an organisation in an inspiring manner.[35]

References

Article 29 Working Party: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is" likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01. http://ec.europa.eu/newsroom/article29/item-de-tail.cfm?item_id = 611236. Accessed 15 Apr 2018

Acquisti, A., Friedman, A., Telang, R.: Is there a cost to privacy breaches? an event study. In: ICIS 2006 Proceedings, p. 94 (2006). http://aisel.aisnet.org/icis2006/94. Accessed 16 Apr 2018

[35] The RESPECT4U white paper outlines the basic elements of the RESPECT4U privacy principles. See https://pilab.nl/research/respect4u.html/; last accessed 2018/05/21.

Aquisti, A.: Nudging privacy – the behavioral economics of privacy. In: IEEE Privacy & Security, November/December, pp. 72–75 (2009)
Acquisti, A., Taylor, C., Wagman, L.: The economics of privacy. J. Econ. Lit. **54**(2), 442–492 (2016)
Barker, K., et al.: A data privacy taxonomy. In: Sexton, A.P. (ed.) BNCOD 2009. LNCS, vol. 5588, pp. 42–54. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-02843-4_7
Baduri, G., Ha-Brookshire, J.E.: Do transparent business practices pay? Exploration of transparency and consumer purchase intention. Cloth. Text. Res. J. **29**(2), 135–149 (2011)
Bennet, C.J., Raab, C.D.: The Governance of Privacy. The MIT Press, Cambridge/London (2006)
Bost, R., Popa, R.A., Tu, S., Goldwasser, S.: Machine learning classification over encrypted data. Crypto ePrint Archive (2014). https://eprint.iacr.org/2014/331.pdf
Cavoukian, A.: Privacy by Design – The 7 Foundational Principles (2011). https://ipc.on.ca/wp-con-tent/uploads/Resources/7foundationalprinciples.pdf
Colesky, M., Hoepman, J.-H., Hillen, C.: A critical analysis of privacy design strategies. In: IEEE Security and Privacy Workshops (SPW) (2016). https://doi.org/10.1109/spw.2016.23
Council of Europe: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strassbourg (2013)
Danezis, G., et al.: Privacy and Data Protection by Design – from policy to engineering. ENISA (2014)
De Vos, H., et al.: 16244 – PIME - A1602, Guidelines on inclusion of users' perception and attitude on offering control and choice with respect to health data and health data services, EIT PIME Deliverable 2 (2016)
Eggert, E., Helm, S.: Exploring the impact of relationship transparency on business relationships: a cross-sectional study among purchasing managers in German. Ind. Mark. Manag. **32**(2), 101–108 (2003)
Executive Office of the President: Big Data: A Report on Algorithmic Systems, Opportunity and Civil Rights, US Presidency (2016)
Erikin, Z., Veugen, T., Toft, T., Lagendijk, R.L.: Generating private recommendations efficiently using homomorphic encryption and data packing. IEEE Trans. Inf. Forensics Secur. **7**(3), 1053–1066 (2012)
Finn, R.L., Wright, D., Friedewald, M.: Seven types of privacy. In: Gutwirth, S., Leenes, R., De Hert, P., Poulett, Y. (eds.) Data Protection: Coming of Age. Springer, Dordrecht (2013). https://doi.org/10.1007/978-94-007-5170-5_1
Jentsch, N., Preibusch, S., Harasser, A.: Study on monetizing privacy – an economic model for pricing personal information. ENISA (2012)
Galic, M.: Covert surveillance of privileged consultations and the weakening of the legal professional privilege. Eur. Data Prot. Law Rev. **4**, 602–607 (2016)
Gellert, R., Gutwirth, S.: The legal construction of privacy and data protection. Comput. Law Secur. Rev. **29**, 522–530 (2013)
Hildebrandt, M.: Smart Technologies and the End(s) of Law. Edward Elgar Publishing, Cheltenham, Northampton (2015)
Keymolen, E.: Trust on the line – a philosophical exploration of trust in the networked era. Erasmus University, Rotterdam (2016)
Kumaraguru, P., Cranor, L.F.: Privacy Indexes: A Survey of Westin's Studies, CMU-ISRI-5–138, Carnegie Mellon University (2005)
London Economics: Study on the Economic Benefits of PET; Study for the European Commission, DG Justice, Freedom and Security. EC, Brussel (2010)

Paulk, M.: Capability maturity model. In: J.-J. Macinaik (ed.) Encyclopedia of Software Engineering, Wiley Online Library (first published 2002). https://onlineli-brary.wiley.com/doi/book/, https://doi.org/10.1002/0471028959. Accessed 15 Apr 2018

Palmer, J.W., Bailey, J.P., Faraj, S.: The role of intermediaries in the development of trust on the www: the use and prominence of trusted third parties and privacy statements. J. Comput.-Mediat. Commun. **5**(3) (2000). https://doi.org/10.1111/j.1083-6101.2000.tb00342.x. Accessed 15 Apr 2018

Stone, M.: The new (and ever-evolving) direct and digital marketing ecosystem. J. Direct, Data Digit. Mark. Pract. **16**(2), 71–74 (2014)

Saunders, J., Hunt, P., Hollywood, J.S.: Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot. J. Exp. Criminol. **12**(3), 347–371 (2016)

Steen, M., Van der Poel, I.: Making values explicit during the design process. IEEE Technol. Soc. Mag. **31**(4), 63–72 (2012)

Turilli, M., Floridi, L.: The ethics of information transparency. Ethics Inf. Technol. **11**(2), 105–112 (2009)

Youyou, W., Kosinski, M., Stillwella, D.: Computer-based personality judgments are more accurate than those made by humans, PNAS (2015). https://doi.org/10.1073/pnas.1418680112. Accessed 15 Apr 2018

Van den Broek, T., Ooms, M., Friedewald, M., Van Lieshout, M., Rung, S.: Privacy and security – citizens' desires for an equal footing. In: Friedewald, M., Burgess, J.P., Cas, J., Bellanova, R., Preissl, W. (eds.) Surveillance, Privacy and Security, pp. 15–35. Routledge, Abingdon, Oxon/New York, (2017)

Van der Hoven, M.J., Lokhorst, G.J., Van de Poel, I.R.: Engineering and the problem of moral overload. Sci. Eng. Ethics **18**(1), 153–155 (2012)

Van der Hoven, J., Manders-Huits, N.: Value sensitive design. In: Berg Olsen, J.K., Pedersen, S. A., Hendricks, V.F. (eds.) A Companion to the Philosophy of Technology, Wiley Online, Chapter 86, https://doi.org/10.1002/9781444310795.ch86. Accessed 16 Apr 2018

Verheul, E., Jacobs, B.: Polymorphic encryption and pseudonymisation in identity management and medical research. NAW **5/18**(3), 168–72 (2017)

Veugen, T., De Haan, R., Cramer, R., Muller, F.: A framework for secure computations with two non-colluding servers and multiple clients, applied to recommendations. IEEE Trans. Inf. Forensics Secur. **10**(3), 445–457 (2015)

Wright, D., De Hert, P. (eds.): Privacy Impact Assessment, Law, Governance & Technology Series, vol. 6. Springer, Heidelberg (2012). https://doi.org/10.1007/978-94-007-2543-0