RESPECT4U

TNO innovation for life

AUTEUR(S)

Marc van Lieshout
Somayeh Djafari
Petra Vermeulen

Projectname RESPECT4U
Projectnumber 060.24401

CONTENTS

INTRODUCTION

PRIVACY IS BECOMING A BUSINESS ASSET. A NUMBER OF DEVELOPMENTS CONTRIBUTE TO THIS REPOSITIONING OF PRIVACY. IN THE FIRST PLACE, THE EXTREME GROWTH IN THE CREATION OF DATA IN THE PAST FEW YEARS MAKES THE PROTECTION OF PERSONS IN RELATION TO THE PROCESSING OF THEIR DATA MORE RELEVANT. SECONDLY, THE ADVENT OF NEW SERVICES THAT ARE LARGELY BASED ON THE PROCESSING OF (PERSONAL) DATA HAS A MAJOR IMPACT ON THE ORGANISATION OF ENTIRE BUSINESS SECTORS. THIRDLY, THE EMERGENCE OF THE INTERNET OF THINGS FURTHER ENHANCES THE DEVELOPMENT OF NEW PERSONALISED SERVICES, REQUIRING MORE DEDICATED STRATEGIES TO COPE WITH THE DATA NEEDED TO OFFER THESE SERVICES. AND FINALLY, THE RISE OF ADVANCED MACHINE LEARNING TECHNIQUES INDUCES UNFORESEEN CORRELATIONS BETWEEN SEEMINGLY UNRELATED DATA EVENTS AND, WHILE OFFERING MANY CHANCES FOR ENHANCED KNOWLEDGE CREATION IN MANY DOMAINS, MAY AS WELL LEAD TO ADVERSE IMPLICATIONS SUCH AS DISCRIMINATION, UNFAIR TREATMENT AND EXCLUSION OF CLIENTS AND CUSTOMERS.

In this Paper TNO elaborates a number of principles that help organisations to reap the benefits of the sketched developments while respecting the privacy of data subjects. Together, the principles inform an organisation on what it can do to responsibly process personal data: combining secure data processing with full transparency about goals and purposes of data processing.
The principles embed the requirements posed by the EU General Data Protection Regulation. The GDPR is the successor of the Data Protection Directive (DPD) and will be the prime privacy framework of the EU from 25 May 2018 onwards. Being a Regulation, it has enforcing power in all Member States and is implemented 'as is' in all Member States. It introduces rights to data subjects, obligations to controllers and processors, requirements for fair and lawful data processing, and an institutional structure concerning supervision. It embeds novel elements, such as a Data Protection Impact Assessment, Data Protection by Design and by Default, and additional rights to data subjects such as the right to data portability, the right to be forgotten and the right to receive an electronic copy of one's data.
The main thrust of the GDPR is lending responsibility to the organisations themselves in coping with privacy. Self-regulation and accountability are the two key assets of the GDPR. The space to manoeuvre for organisations has increased but in all circumstances organisations should be able to demonstrate that they have adopted appropriate organisational and technical measures to protect the privacy of data subjects.

The Privacy & Identity lab, a collaboration between three Dutch knowledge institutes Radboud University, Tilburg University and Research and Technology Organisation TNO, contributes to the development of privacy respecting measures. The challenge for organisations to cope with the new Regulation in the perspective of the developments briefly sketched is of prime concern for the PI.lab. TNO, focusing on applied knowledge, has used the window of opportunity the adoption of the GDPR offers. It has developed a set of privacy principles and has brought these together in a framework labelled RESPECT4U. This framework concisely presents an overview of the privacy challenges an organisation faces when processing personal data.

The RESPECT4U principles use the GDPR as the legal 'backbone'. Protecting persons in respect to the processing of their data requires a holistic approach in which various perspectives are elaborated and combined. Data need

to be securely processed, privacy risks need to be identified, organisations need to demonstrate accountability. While privacy is often considered to be a dissatisfier, an asset with costs and no revenues, the RESPECT4U principles presume privacy to contribute to customer satisfaction, to help organisations in creating business value and to contribute to lowering organisational costs by dealing with risks in a systematic and structured manner. Considering that the developments taking place today may have unknown, unintended and unforeseen consequences for human values associated with privacy such as discrimination, exclusion, stigmatisation, REFLECT4U includes an ethical perspective as well.

HOW TO READ

In the next chapter we will present the mission and the vision of the RESPECT4U approach. The principles are concisely presented. Then each principle is elaborated by sketching the background of the principle, the perspectives of the expected impact and the measures to concretise the principle. Each chapter succinctly presents an overview of PI.lab activities related to the principle. Main concepts of the GDPR are briefly exposed to give the interested reader some background on the legal framework which RESPECT4U takes into account.

MISSION AND VISION OF RESPECT4U

MISSION STATEMENT

The mission of RESPECT4U is to enable people to act as free and autonomous individuals and to protect them against unreasonable constraints in the creation of their identity.[1] This 'definition' of privacy is just one out of many. It emphasizes several aspects we consider to be relevant in today's data society: autonomy and freedom as core principles of a democratic society in which citizens are enabled to live the lives they want within the boundaries posed by societal norms and regulations agreed upon in a democratic process; the obligation of governments to protect their citizens (classic rights) while offering opportunities to develop themselves (social rights). In a globalising world these protective boundaries and constraints require dedicated attention; they have increasingly become the result of the interplay between public and private actors. The emergence of a data-economy has created additional challenges in which global actors increasingly determine local services and applications on the basis of personal data.

We consider privacy not only to be a core personal value but to be of immanent societal value as well. We want to promote both perspectives through RESPECT4U. The on-going connection between virtual and physical space, reflected in hybrid service provisioning with physical and virtual dimensions, offers enormous opportunities for improved service delivery, be it in health care, in education, mobility or energy. Human beings not only act as the consumers adopting the new services but increasingly become the constituent components of these services, at least in respect to the data they offer that enable these services. This places data subject in an interesting position to negotiate specific features of these services and the use of their personal data for these services. RESPECT4U intends to bridge reasonable expectations of data subjects on a responsible processing of their data with the potential of the newly to deploy services, processes and systems. Data driven innovations help meeting societal demands. The challenge is to align them with privacy safeguards that help promoting a responsible processing of these data.

We will accomplish this mission by:

- Exercising strong and innovative leadership to the privacy of all Europeans.
- Rigorously pursuing excellence in the design and manufacture of processes, tools and instruments that can help organisations to meet the demand of their clients and customers by embedding the highest privacy quality standards available.
- Providing the highest quality educational materials to public and private organisations alike so they know how to best apply and make use of the RESPECT4U-guidelines and principles, aimed at promoting free and autonomous individuals and to reduce significant risks to the protection of individuals, in particular with regard to online activity.
- Disseminating our knowledge, findings and experiences in a free and open manner so that all interested organisations can assess the relevance of our perspectives for their own practices.

VISION STATEMENT

Europeans have always cherished their privacy. The individual and social values embodied by privacy have been supportive to the European

1 P. Agre and M. Rotenberg, Technology and Privacy: The New Landscape, MIT Press, 1997

ideal of free and responsible citizens. Over the years these values have become part of a European approach of creating safeguards by legislation. From the birth of the rule of law, we assured ourselves protection against unlawful intrusion into our homes and our personal letters. And after, we extended privacy protections to new modes of communications such as telephone, computer and eventually email.

Interestingly, the roots of contemporary perspectives on privacy stem from a privacy intrusion by a photo camera in the United States of America. In a famous plea at the end of the 19th century, US-based lawyer Louis Brandeis taught us that privacy is the "right to be let alone". This approach was reflected in the 1948 Universal Declaration of Human Rights that lend each individual an inalienable right to the protection of private and family life, the home and correspondence. These rights are part of the European Charter of Fundamental Rights as well. The right on privacy is complemented with a right on the protection of persons with respect to the processing of their data, a right that is covered by the GDPR. We embrace the interplay between both rights. Everyone who feels protected from misuse of his or her personal data will feel free to engage in commerce, to participate in transactions and communications with each other, or to make use of public services, such as health care, without reserve. This is why we have laws which protect privacy and which protect consumers against unfair and deceptive uses of their personal data.

Never has privacy been more important than today, in the age of big data, internet of things and artificial intelligence. In the last decade, the internet has enabled a renewal of direct commercial engagement by consumers around the globe and an explosion of commerce and innovation creating jobs of the future. Much of this innovation is enabled by novel uses of personal data. So, it is incumbent on us to preserve a collective value whilst enabling the adoption of the fruits of progress: apply our timeless privacy values to the new technologies and circumstances of our times.

One thing should be clear, even though we live in a world in which we share personal data more freely than in the past: we must reject the conclusion that privacy is an outmoded value. It has been at the heart of our democracy, it reflects deeply felt public and personal values from its inception, and we need it now more than ever.

4U

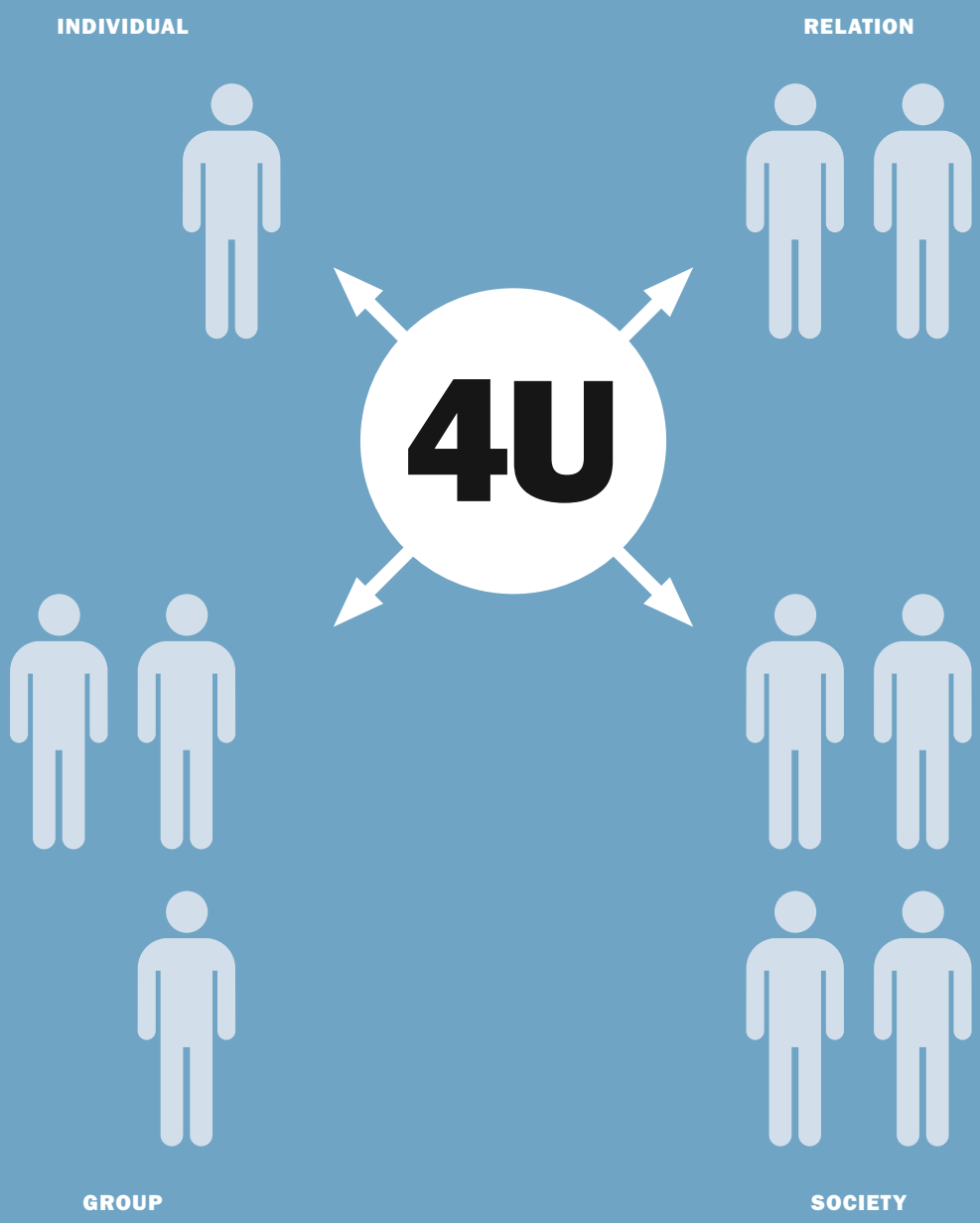
Privacy and the protection of persons with respect to the processing of their personal data reflects the individualistic and atomistic nature of privacy protection. But they reflect a societal value as well, enabling individuals to develop as autonomous and responsible citizens in society. We embed this societal value of privacy in the use of the well-known acronym '4U'. For us, '4U' is not only an easy shorthand writing that reflects popular use of language and symbols. The interpretation goes deeper. One U is the individual, whose claim to privacy is undisputed. Two U's refer to the relationship with the intimate others, the sphere of family, friendship and self-chosen others. Three U's reflect the crowd, the manifold that can be self-chosen but is not under full control of the individual. Four U's reflect a crowd of crowds, a society, in which norms and regulations help keeping democratic principles of justice, fairness, equal treatment and the like upright. RESPECT4U aims to cover the values of privacy and the protection of persons with respect to their personal data in all four domains, aiming to protect the individual, the intimate relations between individuals (as reflected in the home, family life and correspondence), the crowd (as in freedom of association and of expression) and society as a whole (that presumes free and autonomous individuals).

RESPECT4U

Figure 1: The RESPECT4U principles

Figure 1 shows in one glance the seven principles RESPECT4U is based upon. Each principle corresponds with a specific perspective and is elaborated in a number of distinct measures.

- RESPECT4U is related to being 'Responsible': moving away from 'efficient', 'fast', 'cheap' and 'more', towards 'sustainable, 'safe', 'inclusive' and 'privacy respecting'. It is about enabling organizations to demonstrate ability and willingness to act in a privacy respectful manner and to demonstrate accountability for their acts.
- The second principle is about 'Empowerment': giving individuals meaningful instruments to exert influence on what is processed, for which purposes, by whom and under what circumstances. This includes data supervision by individuals, and giving them – some – control over their data.
- 'Secure' means using appropriate technical and organizational means to secure data, to secure the access to data and to secure the processing of data. Novel and innovative techniques help achieving a high level of data security.
- The principle of 'Pro-active' includes anticipation on privacy risks and integrating Privacy by Design and Privacy by Default in the design processes of new data driven products and services.
- Acting 'Ethically' is about creating awareness for the unintended consequences of one's actions and of the hidden assumptions in the algorithms and/or hidden deficiencies in the data processing. It relates to preventing unfair treatment, discrimination, exclusion and stigmatization, the potentially adverse effects of using algorithms which are non-deterministic by nature and thus hard to unravel and understand.
- RESPECT4U includes a principle on identifying costs and benefits associated with privacy. Material and non-material aspects of costs and benefits are often hard to capture: while an organisation may experience material costs in safeguarding personal data, it may as well acquire material benefits because of a better and transparent organisation of its data processes, meanwhile reducing risks on data breaches as well. Clearly not all costs and benefits are entirely material in nature.
- Finally, RESPECT4U is about being 'Transparent': being clear on how internal roles and responsibilities concerning the processing of personal data is organized, how identity and access management is organized, how personnel is held accountable for acting privacy respectful, how organizational processes are influenced through privacy by design/default principles, how audits and privacy checks are implemented.



PRIVACY AS INDIVIDUAL AND SOCIETAL VALUE

RESPONSIBLE

RESPONSIBLE
Starting point is the responsible processing of personal data. An organisation is willing to demonstrate how it has organised its processing of personal data and accepts responsibility and accountability for this processing.

BACKGROUND

The data economy is becoming a major pillar under today's society. Personal data are used for a variety of services and products. These services help meeting societal challenges such as improving health, energy and mobility and offering citizens unprecedented opportunities to engage with each other.

The downside is the loss of control over one's data, and the potential intrusion in one's personal life with chilling effects on one's behaviour and expressions. To counter these potential threats today's data society requires organisations who are willing to expose their intentions and are willing to demonstrate how they fulfil them. Responsible processing of personal data then becomes a corner stone of creating trust.

PERSPECTIVE

One can notice a shift away from organisational approaches that merely focus on being efficient, cheap and fast towards approaches which also have an eye for being sustainable, safe, inclusive and privacy respecting. In the longer term we expect the latter societal norms to become more relevant than the purely business oriented norms. We also expect that organizations will not only act along these lines but are also willing to demonstrate that they do so.

WHAT TO DO

Responsible behaviour in relation to the processing of personal data and safeguarding the privacy of customers can be demonstrated in a variety of ways. Organisational instruments are the establishment of a Data Protection Officer, the adoption of a Code of Conduct, the introduction of Certification Schemes apt for the purpose, the publication of an Annual

The PI.lab has played a prominent role in the activities of the Dutch expert group on Big data and privacy. This expert group has been commissioned by the Dutch department of Economic Affairs. It has advised the minister of Economic Affairs on the reconciliation of innovation with privacy in times of big data. It has published its findings in the report 'Light on the Digital Shadow' (Dutch only).

Privacy Report, the creation of a Critical Panel of customers, and the adoption of specified Audit principles.

PERSONAL DATA

The General Data Protection Regulation deals exclusively with data concerning natural persons. The concept 'personal data' should be interpreted in a broad manner: all data that directly or indirectly identify a natural person are considered to be personal data. The name of a person is a trivial example of directly identifiable data. But also a licence plate or an IP-address are personal data. The IP-address and the licence plate enable the indirect identification of a natural person, for instance through relating these data to the owner of a computer respectively the owner of a car. The same goes for pseudonymous data, an identifier that replaces a name of a person. The identifier indirectly identifies a natural person. All these data are personal data and thus are covered by the GDPR.

EMPOWERING

BACKGROUND

As ordinary citizens, as customers involved in a transaction we give away data without exactly knowing why and what happens with these data. Though legal prescriptions enforce all kind of obligations on those processing our data, in reality this hardly offers satisfactory solutions. Surveys demonstrate that people increasingly become aware of and worried about the lack of control over their own data, with potentially negative impacts on their willingness to share data for beneficial purposes. From a social, economic ànd individual perspective, empowering the data subject such that s/he is able to exercise some kind of control will promote willingness to share data, enhance trust and thus contribute to a mature and inclusive service economy that is largely based on personal data.

PERSPECTIVE

Empowerment is an essential step in becoming privacy respecting, as it gives individuals recognition of their role in the data economy. It acknowledges the fundamental rights set in the physical world as being relevant in the digital world as well. However, there is no “one size fits all” policy in empowering individuals. Differentiation in how empowerment is organized is crucial: some want to have full control, others will be happy when they can rely on the judgement of a trusted institution or instrument that informs them and keeps control on behalf of them. The starting position is presented by the rights given to data subjects in the General Data Protection Regulation. Empowerment goes beyond merely exerting influence: it has an inherent element of being able to live as a fully autonomous and respected individual.

WHAT TO DO

Instruments to ensure rights of those involved can be grouped together in a Privacy Dashboard. A privacy dashboard serves a number of purposes: it informs individuals on what data are processed and for which purposes, it informs them on the organization of data processes within an organization and the distribution of responsibilities (see also Transparency). Secondly, a Privacy Dashboard may offer some kind of control to individuals, enabling them to determine which data can be processed for which purposes (right to object against the processing of data). This feature shall have to be contextually implemented: sometimes control can be exerted without constraints, in other situations legal or contractual obligations may play a role. Other rights that can be implemented in a privacy dashboard are the right to rectify incorrect, outdated or irrelevant data, the right to data portability, the right to be forgotten. Some of these rights are new (data portability, the right to be forgotten) and some of them can only be invoked under specific conditions (right to data portability).

Finally, and becoming increasingly relevant, is the right to be informed about the logic behind decisions made which have significant or legal implications for the individual, and – as part of this – the right to know how a profile about a person has been constructed (profile transparency).

PROCESSING OF DATA

The GDPR deals with processing of personal data. The concept 'processing' should be interpreted broadly. It covers all activities that are executed on data, such as collecting, storing, analysing, disseminating, removing, distributing, archiving and destroying.

The PI.lab presumes individuals to have different preferences concerning their control over their data. The PI.lab partner TNO develops a privacy dashboard for health care in which different approaches are embedded.

SECURE

SECURE
Personal data need to be securely stored and processed. Access to personal data needs to be strictly organised and controlled. Advanced and innovative technical and organisational measures support secure storing, processing and accessing personal data.

BACKGROUND

Data are becoming the core asset of organisations today. The secure storage and processing of data becomes a relevant key performance indicator that – if not fulfilled – may lead to sincere negative impacts on the organisation's operations. The reputation of organisations that have been confronted with a data leakage or a data hack is seriously inflicted with potentially long-term consequences for the credibility of the organisation. On the other hand, a secure handling of personal data contributes to lending credibility to an organisation.

PERSPECTIVE

Security of data consists of three parts: securing the data, securing access to the data, and securing the processing of data. Together the measures undertaken to achieve this, form the appropriate technological ànd organisational measures the data protection directive and the GDPR require. Security technologies have evolved over the past decades and enable sophisticated management and processing of encrypted data. Access management strategies have evolved that make use of intelligent protocols and organisational models.

WHAT TO DO

On the technological side a variety of encryption protocols have been developed. Secure multi-party computation, homomorphic encryption and polymorphic encryption and pseudonymisation are sophisticated protocols

Secure access
- Acces control
- Audit control
- Encryptie
- Identity and access
- Management
- Facility Access Controls
- Workstation security
- Signing and verifying

Secure data
- Homomorphic encryption
- Hashing
- Watermarking
- Steganography

Secure processing of data
- Attribute based credentials
- Polymorphic encryption and pseudonimisation
- Homomorphic encryption
- Anonymisation
- Pseudonymisation

PI.lab partners Radboud University and TNO work on advanced cryptographic protocols that enable fine-grained access to personal data and that enable secure processing of personal data while still encrypted.

that help organising data processing without jeopardizing integrity of data. The complexity of these protocols has not been sufficiently mastered today to enable widespread use, but it is expected that the protocols will mature over the years to come to ready business applications. Encryption tools such as homomorphic encryption enable to perform transactions on data while these data remain encrypted. Sophisticated key management systems have evolved as well, including personal data vaults and systems using attribute based credentials for organising data exchange. Attribute based credential systems help organising data processes such that a minimal set of data is released to fulfil a specific service. Identity and authentication access management systems complete the technical and organisational toolbox for secure data handling.

PURPOSE AND LAWFULNESS OF PROCESSING

Before processing data of natural persons, the controller needs to present a purpose and needs to show the lawfulness of processing. The purpose needs to be legitimate, specific and explicit. The lawfulness of the processing covers six possible grounds:

1. Freely given, specific and informed consent of the data subject
2. Fulfilment of contractual obligations
3. Fulfilment of legal obligations
4. Vital interest of the data subject
5. Public interest
6. Legitimate interest of the controller or a third party

When personal data will be processed for a new purpose, one needs to determine the compatibility of this new purpose with the original one. In case the new purpose is not compatible with the original purpose, the lawfulness of processing needs to be determined again. Compatible use depends on scope, nature of personal data processed, context and consequences of processing.

PRO-ACTIVE

PRO-ACTIVE
An organisation understands the privacy risks of its products and processes. Securing privacy is taken into account from the very first beginning of the design of new systems, products and processes.

BACKGROUND

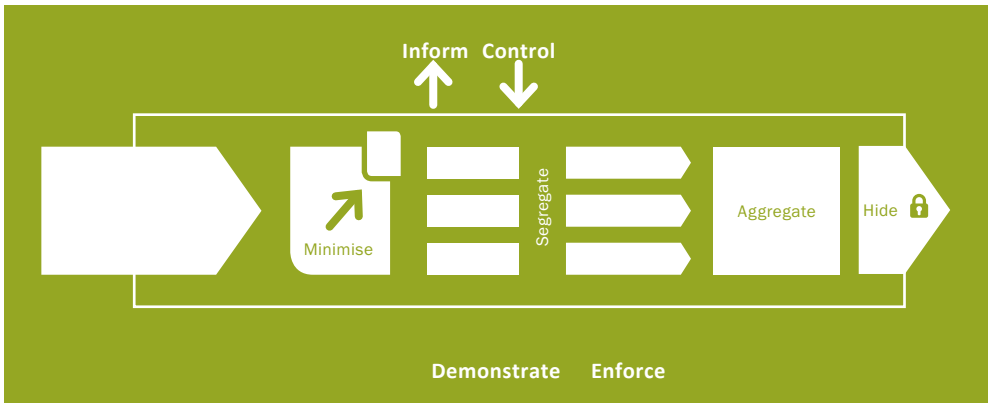
"An ounce of prevention is worth a pound of cure." This famous saying by Benjamin Franklin is not just applicable in the physical world but in the online world as well. An assessment of privacy risks before systems are developed enables an encompassing approach to privacy as an integral part of systems design, development and use. In line with Franklin's saying this offers benefits both in operational costs and in prevention of dramatic losses of data or inflictions on privacy with potentially large adverse implications for individuals and negative impacts on the reputation of the organizations involved.

PERSPECTIVE

A pro-active attitude oriented towards inventorying privacy risks, developing a strategy to include privacy by default and privacy by design from the early start of systems design enables organizations to capture the benefits of a privacy respecting approach at minimal costs. The encompassing approach is a combination of the use of the Privacy Maturity Model (PMM) and the application of a Privacy Impact Assessment. The operational part is offered by privacy by design strategies which are becoming available.

WHAT TO DO

Any pro-active strategy starts by inventorying risks to mitigate. A Privacy Impact Assessment is the tool that enables organisation to assess the risks their data processing activities may evoke and helps establishing measures to



Reseachers of the PI.lab work on a systematic and structured approach of Privacy by design strategies and partners. See https://www.cs.ru/~jhh/publications/pdp.pdf

cope with identified risks. Though not standardised yet, PIAs have been developed in various forms to support organisations in mapping the privacy risks they need to counter. They differ from liability assessments in that the focus is on the risks for the data subject, and not on the liability risks for the organisation. In developing new systems, Privacy by design strategies and patterns can be invoked, supportive to the idea of protecting privacy throughout the process of system design and development, from the conception of a new service or product up to its realisation. The GDPR mentions data minimisation and pseudonymisation as key instruments for privacy by design. Privacy by default is another striking approach that forces organisations to think in terms of privacy features to be offered as default parameter instead of as choice. Having privacy as an integral part of the development process, the final product embeds privacy features throughout its entire life cycle.

PSEUDONYMISED AND ANONYMISED DATA

Anonymised data are not considered to be personal data anymore. It is not possible to directly or indirectly identify a natural person on the basis of anonymised data. The GDPR thus does not apply on anonymised data. Novel developments in analysis technologies enable however the screening and correlation of large heaps of data, leading to the re-identification of natural persons. Several studies show the power of re-identifying natural persons from data that are considered to have been sufficiently anonymised. Practically, real anonymization is very hard to achieve. The GDPR states that the costs in time and resources (money, techniques) that are needed to re-identify a person on the basis of anonymised data determines whether the data can be considered to be sufficiently anonymised. The Article 29 Working Party has indicated which techniques can be considered to be sufficiently anonymising (Opinion 2014/5).

A more reasonable approach than relying on anonymization is to pseudonymise data such that re-identification becomes difficult as well. Pseudonymised data still are considered personal data but proper pseudonymization drastically enhances the protection of personal data. The GDPR consequently refers to pseudonymization as technique to be used for securing personal data.

ETHICAL

ETHICAL

New forms of unfair treatment, exclusion and discrimination are popping up. Advanced AI-based algorithms are sometimes hard to understand and explain. New approaches need to be developed that help coping with new ethical issues.

BACKGROUND

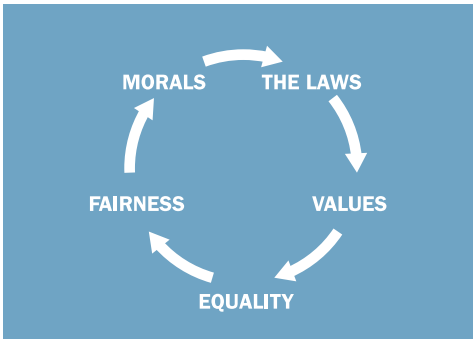
Today's data driven innovations impact upon many facets of daily life. As stipulated in the previous items, many of these impacts can be countered by pre-emptive measures. But it becomes ever more clear that not all impacts can be assessed pro-actively. Even when paved with good intentions, data analytics may turn out to have unwanted and unintended consequences which seriously impact specific individuals or groups of individuals. This may be caused by flawed data collection practices that experience deficits or biases in data collection strategies. It also may be caused by using data analytics approaches, such as machine learning techniques, that intrinsically are subject to non-deterministic behaviour. The consequences of this all may be that data services promote discrimination, exhibit exclusion of specific groups of individuals or show features of unfair treatment. This may cause sincere trust issues in the data processing intentions of organisations and thus warrant precautionary measures.

PERSPECTIVE

An organisation should be aware of the potentially detrimental impacts its activities may have due to flaws in data collection and data processing activities. These are hard to generalize issues at this moment in time. When taking resort to advanced machine learning techniques and when using complex data collection strategies, organisations should be aware of potentially negative consequences such as discrimination, exclusion, stigmatisation and unfair treatment. Even when not intended, these consequences may occur due to the used data collection strategies and machine learning techniques, This may sincerely refute the reputation of organisations.

WHAT TO DO

Organisations can use an ethical impact assessment, that assesses the ethical consequences of specific processing activities. Such an ethical assessment can focus on uncertainties and indeterministic features of advanced algorithms in order to chart



All PI.lab partners study emerging technologies and their potential ethical implications. They focus on inventorying and understanding new risks and developing new coping strategies.

potentially undesired or discriminating outputs. It can also focus on long-term consequences (such as 'chilling effects') that may be induced by wide-spread use of specific data driven innovations. Involvement of data subjects in these assessments lend credibility to these exercises and may bring forward hidden assumptions and expectations. Special attention should be given to potentially negative consequences for specific subgroups: are there incentives for discrimination, stigmatization or exclusion (for instance because of data bias)? Are sensitive data used that require specific attention?

SCIENTIFIC, HISTORIC AND STATISTIC RESEARCH

When processing personal data for scientific and historic research or statistical purposes the controller may rely on a number of exceptions. The basis for these exceptions is the public interest of scientific and historic research and statistical studies. Statistical results are usually not attributable to individual persons, neither is this the direct goal of much scientific research. Scientific and historic research and research for statistical purposes do not have to demonstrate the lawfulness of processing when data are used that have already been collected. In specific circumstances they also can be exempt of fulfilling rights of data subjects (such as the right of access, rectification and restriction of processing). They still need to take into account measures to protect the interests of persons and they need to be able to demonstrate that they have taken sufficient precautions to prevent misuse and abuse of personal data.

COSTS AND BENEFITS

BACKGROUND

Many organisations perceive privacy as a 'dissatisfier' or compliance item, a feature that will cause negative consequences when not properly dealt with but with no added value from a business perspective. In a similar vein, privacy is considered to act as an innovation 'disabler' instead of enabling innovations. This however, are outmoded views. For one, the relevance of properly taking privacy into account only grows and is becoming a more prominent feature in decisions made by individuals to accept services and to engage in a relationship with the service provider. For another, organising services in a privacy-by-design manner adds business value because it prevents costly repair measures while ensuring security of data and data processes at minimal costs. Novel privacy-driven applications may add business value to services and products offered. In order to make informed decisions on the optimal level of privacy respecting features in one's products and services, a proper cost-benefit analysis is prerequisite.

PERSPECTIVE

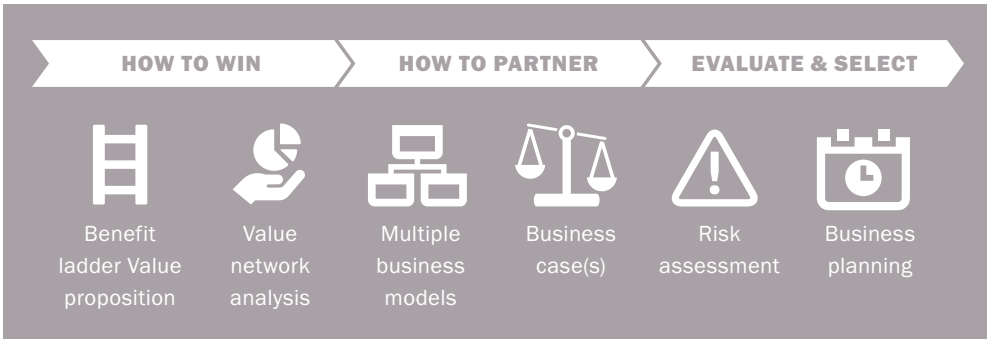
Trying to engage with a cost-benefit analysis, one needs to address costs and benefits in a comparative manner. This by itself poses challenges. Not always are benefits falling towards parties making the costs. Cleaning up the environment for instance, as a sidewise comparison, is a cost-factor for an organisation but a beneficial factor for the citizens living nearby the polluting plant. Sometimes, costs have to be made immediately while benefits only demonstrate in the long run. Costs for installing a separate data protection officer in the organisation, or for implementing a new system that secures data storage can usually be determined a priori. This may be more problematic for benefits. Benefits can be of material and of immaterial kind. Material benefits are the costs saved because of having secure operations, less data, better safeguarding procedures and clear distribution of responsibilities, and thus a lower risk on privacy breaches. Material benefits relate to the preventive aspects of not being fined for data leakage or for not fulfilling requirements of regulations. Immaterial benefits consist of increased trust by clients and a potentially larger client base given positive reputation impacts. The precise scoping of these benefits is hard to tell in advance, while they can be substantial as well.

WHAT TO DO

The most relevant instruments are the cost-benefit analysis (CBA), and Business Modelling, ideally used in combination.

Typically, a CBA follows three distinct steps, that are progressively more complex:

1. Identify and compare scenario's. Ideally, several options will be compared. A scenario may involve choices on technological architecture, governance model, and/or implementation strategy. Just creating a



The PI.lab develops new business models that take privacy into account. It also studies costs and benefits of privacy in organisations.

structured overview of the possible options already greatly improves decision making.

2. Qualify costs and benefits. For each scenario, the costs and benefits need to be detailed at a sufficient qualitative level to give insight in the net-effects of each scenario. Typical approaches to estimate these costs and benefits is by using workshops, Delphi method, and expert opinions.
3. Quantify costs and benefits: Quantifying investment and operational costs related to each scenario is usually relatively straightforward, given an organisation has a good sense of cost allocation, and the scenarios are sufficiently detailed, both in terms of technology as in organisational requirements. The challenging part is quantifying the benefits described in step 2, especially when they are quite abstract, such as “increased customer satisfaction”. Several methods can be used, ranging from formal quantification methods and tools, to creating consensus on easy rules-of-thumb in a workshop business modelling.

Business modelling

Some privacy-related decisions only have effect on the internal organisation. But especially in data-driven innovations, the overall privacy aspects of a certain service are dependent on the interplay of many organisations supplying sub-services that create a final value-proposition to the customer. This especially holds true for cases in which privacy is considered a true value driver for the new service. One then needs to assess the value network and the roles and incentives of the organisations involved. From that starting point, one should identify related business model design consequences, and position this new service in the (business and/or public) ecosystem. Different design choices might affect aspects of the implementing organisation (such as value proposition, resources, channels), but also might affect other organisations within the ecosystem the organisations is operating in. Especially in data-driven innovation, services do not stand alone, but require a complex interplay with services from other organisation in a so called value-network.

Ideally, cost-benefit analysis and business modelling go hand-in-hand in iterating cycles. For different implementations, the total cost might be roughly the same, but the division of costs/benefits over the various roles in the value web can make or break the success of a new service.

TRANSPARENT

TRANSPARENT
Transparency on which data are processed for which purposes. Transparency on roles and responsibilities within an organisation. Transparency on accountability measures.

BACKGROUND

Restoring the present imbalance in which individuals become increasingly transparent to organisations while organisations are rather opaque to individuals means introducing transparency within the organisation.
Many other domains already have organised transparency measures in order to meet societal expectations and quality requirements. Within retail, the food industry and sectors such as the clothing industry quality labels are used that show responsible and fair trade (proper labour conditions, no use of pesticides, sustainable agricultural and energy conditions, etc.). Within the data economy a similar system is yet lacking. Introducing transparency in what is done, for which purpose and with what data, offers added value to demonstrate responsible innovation and entrepreneurship.

PERSPECTIVE

Legal obligations (in the GDPR) require that organisations offer transparency to individuals with respect to the data they process, the purpose for which these data are processed, the rights that individuals can exercise with respect to this processing. Profiling and automatic decision making require specific consent procedures and offer additional guarantees to data subjects. Transparency measures help in meeting these legal requirements and may help in promoting a responsible attitude throughout the organisation. Demonstrating roles and responsibilities within an organisation (who is responsible and accountable for which data processes?) and creating awareness for these roles and

- Data minimisation
- Purpose specification
- Integrity and confidentiality
- Consent
- Legitimate ground for processing
- Privacy by design and by default
- Notification obligation of data breach
- Demonstrating accountability
- Demonstrating appropriate technical and organisational measures

The PI.lab develops instruments that support organisations in demonstrating transparency and accountability.

responsibilities improves transparency towards data subjects and employees. Behaving transparent creates organisations that act predictably, that behave trustworthy and that further a trust relation with their clients.

WHAT TO DO

A responsible processing of personal data requires the involvement of the full organisation. Roles and responsibilities need to be determined and to be attributed. Transparency can be promoted by establishing a transparency dashboard (as part of or in addition to a privacy dashboard; see section on Empowerment). Such a dashboard should indicate the data policy of an organisation (what data are processed, for what purposes, how are rights of data subjects met and how are obligations of the organisation fulfilled). It could be combined with transparency over executed Data Protection Impact Assessments, and over roles and responsibilities.

CONTROLLER AND PROCESSOR

The organisation that determines the purposes and the means of processing is the controller, according to the GDPR. The controller has a number of obligations to fulfil, and needs to be able to demonstrate accountability. The controller can make use of a third party for the actual processing. This party, the processor, is only allowed to do what the controller has instructed the processor to do. A contractual or legal arrangement between the two determines purposes and context of the processing and the instructions for the processing. Controllers can together share responsibility for processing. They then act as joint controllers. Processors can act as controller when processing personal data for purposes not agreed upon with the controller.

NEXT STEPS

In the preceding sections we have presented a large variety of measures an organisation can adopt in order to contribute to a responsible processing of personal data. The baseline of many of these measures is formed by the legal framework that will enter into force 25 May 2018. This framework, the General Data Protection Regulation, stipulates rights of data subjects and obligations of controllers and processors. It does not prescribe in detail how an organisation should meet these rights and obligations. Over the next few years, issues such as what constitutes a proper Data Protection Impact Assessment and what are minimal requirements of Data Protection by Design will be determined in more detail by the European Data Protection Board that will be established as successor of the present-day Article 29 Working Party.

Technical means such as attribute based credential systems, novel encryption technologies and privacy respecting identity and access management systems are already available and are part of on-going research efforts. Instead of promoting 'add-on' solutions that can 'fix' privacy problems, systems design will have to move towards integrative approaches in which privacy is one of the design parameters that will be taken into account from the early phases of the development of a novel system.

Organisational measures can help promoting a privacy respecting attitude and can offer incentives to employees within an organisation to be aware of privacy issues in their daily activities while being supported by appropriate tools to act accordingly. A Data Protection Impact Assessment is prerequisite for specific data processing activities. It should be used as an instrument that helps identifying privacy risks and that helps organising the organisational approach towards these privacy risks. But instead of using a DPIA as a 'single shot' instrument it can also be inserted into the organisational processes that accompany regular audits and internal check-ups.

Working on these approaches is timely, given the fact that some measures need to have been fulfilled from 25 May 2018 onwards. Of course, taking care of privacy and seeking for ways to contribute to the responsible processing of personal data is not an isolated challenge for organisations that process personal data. It goes hand in hand with heightened attention by branch organisations, supervisory authorities and public authorities that want to organise, exchange and disseminate best practices and offer support in other manners.

The final aim is to meet legal requirements while using the potential of new technologies in order to be responsive to societal needs.

THE PI.LAB

The PI.lab is a collaboration of Radboud University (department Digital Security), Tilburg University (Tilburg Institute for Law, Technology and Society) and TNO (Roadmap Networked Information). The three institutes have combined forces in studying digital privacy and identities with an aim at contribution to proper societal solutions. The three institutes bring together some fifty leading scientists who dedicate their work to studying technical, regulatory, organisational, societal and policy-related challenges concerning digital privacy and identities. The results of their work contribute to supporting clients in innovating their services in a privacy respectful manner.

The PI.lab considers the respectful promotion of privacy as an asset that will help connecting new opportunities provided by new innovations with fundamental rights, thus supporting new services and applications that will benefit all. The PI.lab critically reflects upon the advent of new technologies and their impact upon fundamental rights such as privacy, and contributes in developing new technological and business oriented approaches in encryption technologies, privacy design strategies, and organizational tools and methods to promote and implement privacy respecting products and processes.

Contact
Marc van Lieshout
BUSINESS DIRECTOR PI.LAB
SENIOR RESEARCHER/ADVISOR
STRATEGY & POLICY
Locatie Den Haag – New Babylon
marc.vanlieshout@tno.nl
+31 (0)88 866 71 25
+31 (0)65 124 6618

TNO innovation for life

TNO.NL

17-9539 januari 2018