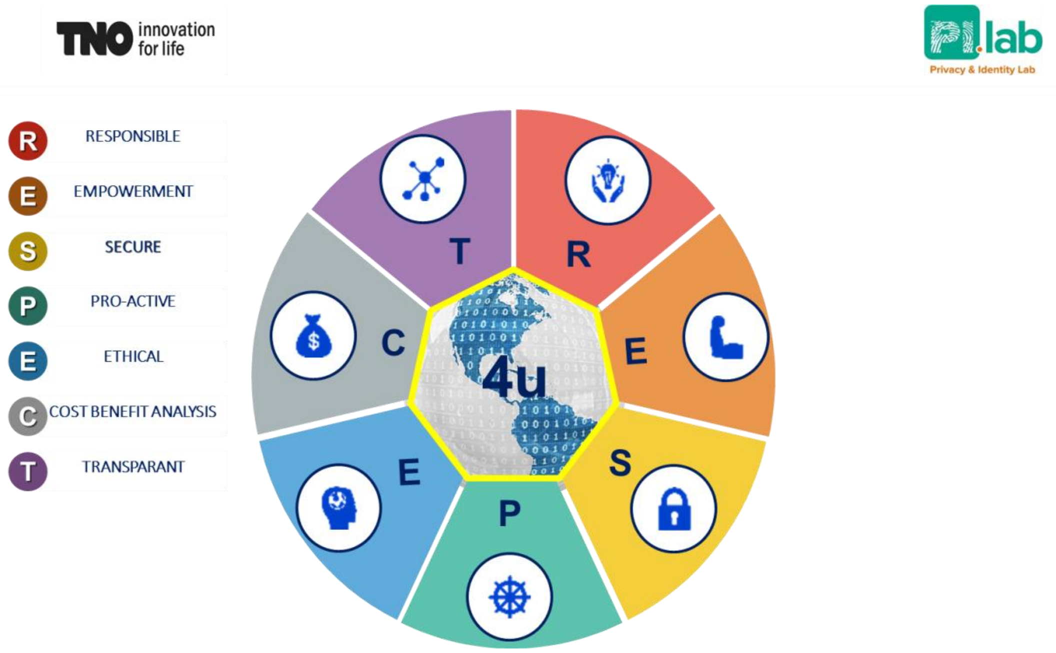
RESPECT4U



Marc van Lieshout, Somayeh Djafari & Petra Vermeulen

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.

The European Union has recently adopted a successor to the Data Protection Directive (DPD). The DPD dates back to 1995 and was basically prepared in the pre-internet era. Its successor, the General Data Protection Regulation, will enter into force 25 May 2018. Being a Regulation it has enforcing power in all Member States in a similar manner. 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 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 present-day developments in combination with the adoption of the GDPR offers. It has developed a privacy framework, labelled RESPECT4U, that concisely presents an overview of the challenges an organisation faces when processing personal data.

The RESPECT4U framework uses 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 framework presumes 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 threats to human values associated with privacy such as discrimination, exclusion, stigmatisation, REFLECT4U includes an ethical perspective as well.

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. This 'definition' of privacy is just one out of many. It emphasizes several aspects we consider to be relevant in today's data society: considering 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 boundaries and constraints have become more subtle and 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 thus 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. We focus on data driven innovations, products and services, these being the most visible form of developments taking place today in which offline and online activities become increasingly intertwined and undiscernible.

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.
- Disseminate 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 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 famous 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”. But we also know that privacy is about much more than just solitude or secrecy. Everyone who feels protected from misuse of his or her personal data feels free to engage in commerce, to participate in transactions and communications with each other, or to seek needed health care. This is why we have laws which protect privacy and which protect consumers against unfair and deceptive uses of their personal data. This is why the court has protected anonymous political speech, the same right exercised by the pamphleteers of the early nations and today's bloggers.

Never has privacy been more important than today, in the age of big data, internet of things and artificial intelligence. In just 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 do what we have done throughout history: 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 is enshrined in various European and international laws and treaties. For the EU most prominent are articles 7 and 8 in the European Charter of Fundamental Rights. While article 7 lends European citizens the right to privacy, article 8 offers similar protection to European citizens with respect to the processing of their personal data.

These articles are often understood as reflecting the individualistic and atomistic nature of privacy protection. But they reflect the societal value of privacy as well, enabling individuals to develop as autonomous and responsible citizens.

We reflect this societal value of privacy in the use of the well-known typography ‘4U’. For us, it 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 shows the various dimensions of RESPECT4U in one encompassing view.

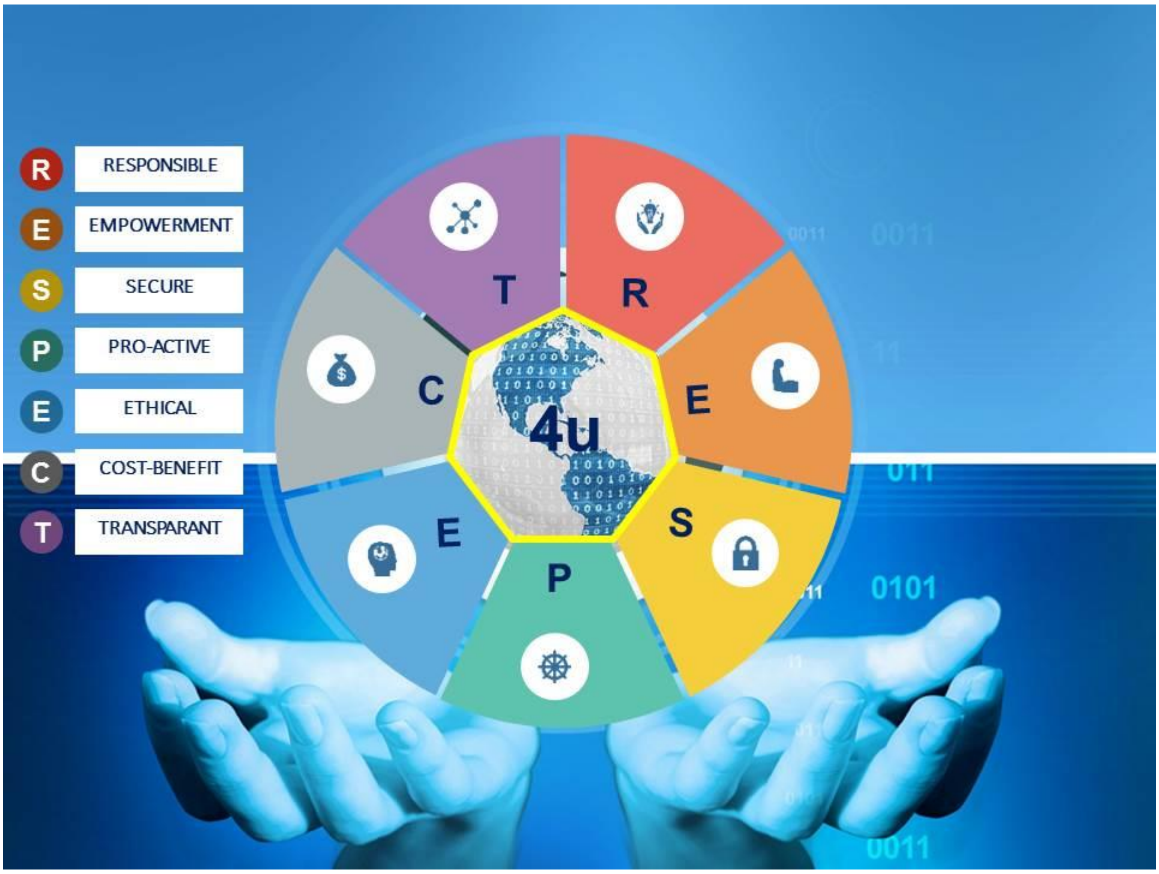


Figure 1: The RESPECT4U framework

The various perspectives of RESPECT4U will be elaborated in the next sections. Each section is subdivided in three subsections, entitled as ‘Why’, ‘What’ and ‘How’.

‘Why’ will present the motivation of having this perspective. Why is it relevant for the protection of privacy?

‘What’ will present the objectives of having this perspective realised.

‘How’ will present the instruments and actions that can be undertaken to realise the objectives.

Wherever possible, we will present examples to illustrate how the perspective is covered in projects we have been engaged with.

Introduction to the various perspectives

The various dimensions are briefly exposed underneath:

- 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.
- It 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 high level of data security.
- Being “Pro-active” includes anticipation on privacy risks and by 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, potentially adverse effects of using algorithms which are non-deterministic by nature and thus hard to unravel and understand.
- RESPECT4U includes a perspective 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 by a better and transparant 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.

Responsible

Why

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.

What

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.

How

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

Responsible

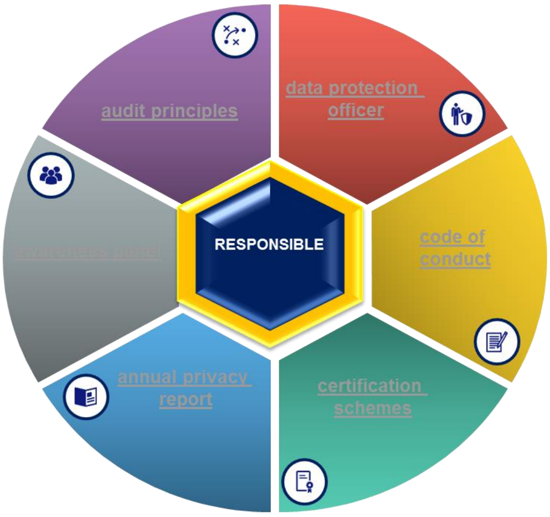


Figure 2: Instruments for acting responsibly

Empowering

Why

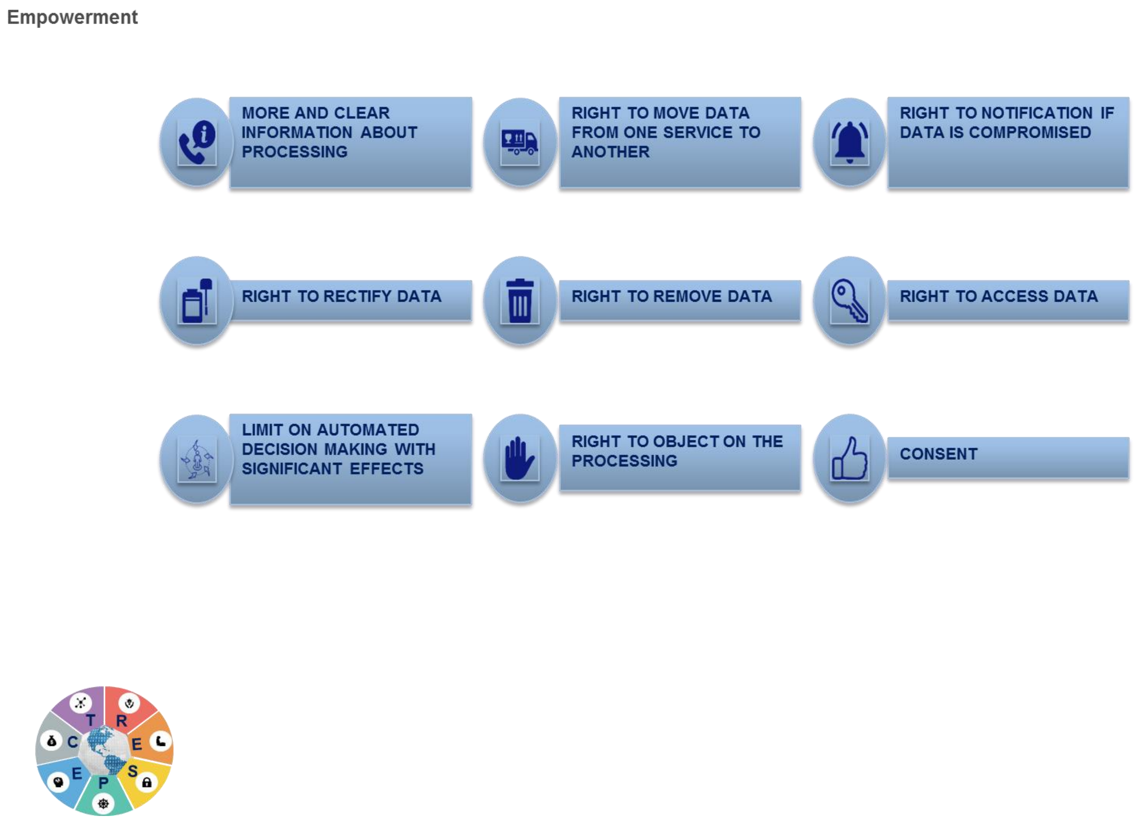
As ordinary citizens, as customers involved in a transaction we give away data without exactly knowing why and what happens with these data. Though legal prescriptions enforce all kind of obligations on those processing our data, in reality this hardly offers satisfactory solutions. Surveys demonstrate 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 further willingness to share data, enhance trust and thus contribute to a mature and inclusive service economy that is largely based on personal data.

What

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 so-called 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.

How

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 cannot always be invoked (right to be forgotten). Finally, and becoming increasingly relevant, is the right to be informed about the logic behind decisions made which have signifcant 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).



Empowerment

MORE AND CLEAR INFORMATION ABOUT PROCESSING

RIGHT TO MOVE DATA FROM ONE SERVICE TO ANOTHER

RIGHT TO NOTIFICATION IF DATA IS COMPROMISED

RIGHT TO RECTIFY DATA

RIGHT TO REMOVE DATA

RIGHT TO ACCESS DATA

LIMIT ON AUTOMATED DECISION MAKING WITH SIGNIFICANT EFFECTS

RIGHT TO OBJECT ON THE PROCESSING

CONSENT

Figure 3: Rights of data subjects that need to be met

Secure

Why

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.

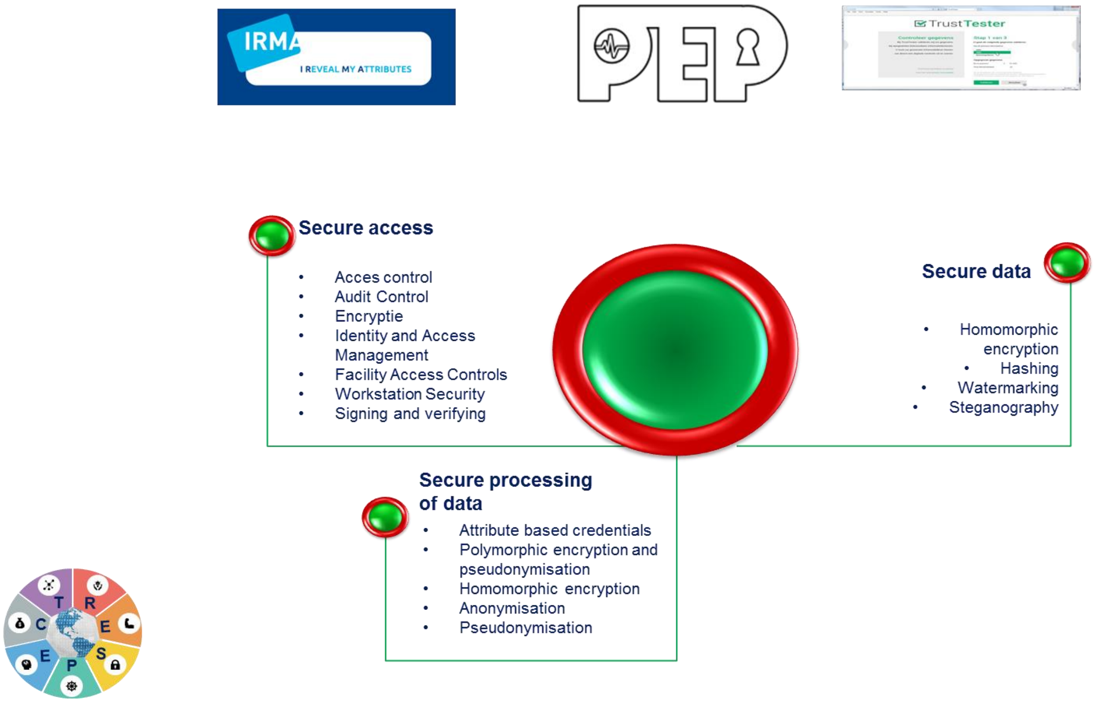
What

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.

How

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

Security



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 pseudonymisation
- Homomorphic encryption
- Anonymisation
- Pseudonymisation

Figure 4: Instruments for making data processing more secure

Pro-active

Why

“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 privacy implications for individuals inflicted and negative impacts on the reputation of the organizations involved.

What

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.

How

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 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 in liability assessments in that the focus is on the risks for the data subject, and not – or less – on the liability risks of 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 business design and development, from the conception of a new service or product up to its realisation. An encompassing approach towards encapsulating Privacy by design strategies is under elaboration, and offers interesting perspectives.[1] 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 is an integral part of the development process, the final product embeds privacy features throughout its entire life cycle. The GDPR mentions data minimisation and pseudonymisation as key instruments for privacy by design. Data minimisation is about which data is collected – it refers “to the practice of limiting the collection of personal information to that which is directly relevant and necessary to accomplish a specified purpose”.[2] In other words, data should be

[1] Jaap-Henk Hoepman, Privacy Design Strategies, via: https://www.cs.ru.nl/~jhh/publications/pdp.pdf

[2] Forbes, Why Data Minimization Is An Important Concept In The Age of Big Data, Bernard Marr, 16 maart 2016. Geraadpleegd op 21-07-2016, via: http://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/#7182cd83327f

“adequate, relevant, and not excessive” in relation to the purpose for which it is processed. Pseudonymisation is about segregating identifying attributes from data records and replacing them with a pseudo-identifier (such as a – randomly chosen – number). Pseudonymised personal data are still to be considered as personal data. This is not the case for anonymised data. Anonymisation is however much more difficult to achieve. Opinion 03/2014 of the Article 29 Working Party presents an overview of measures needed to declare personal data anonymised. Phil Lee captures the difference in by-going quote.

“Using anonymisation, the resulting data should not be capable of singling any specific individual out, of being linked to other data about an individual, nor of being used to deduce an individual's identity. (….) Conversely, pseudonymisation means replacing 'obviously' personal details with another unique identifier, typically generated through some kind of hashing, encryption or tokenisation function. For example, "Phil Lee bought item x" could be pseudonymised to "Visitor 15364 bought item x".

Both of the techniques attest of a pro-active attitude, however, true anononymisation is much harder to achieve, as not a single distinguishing feature can be forgotten.

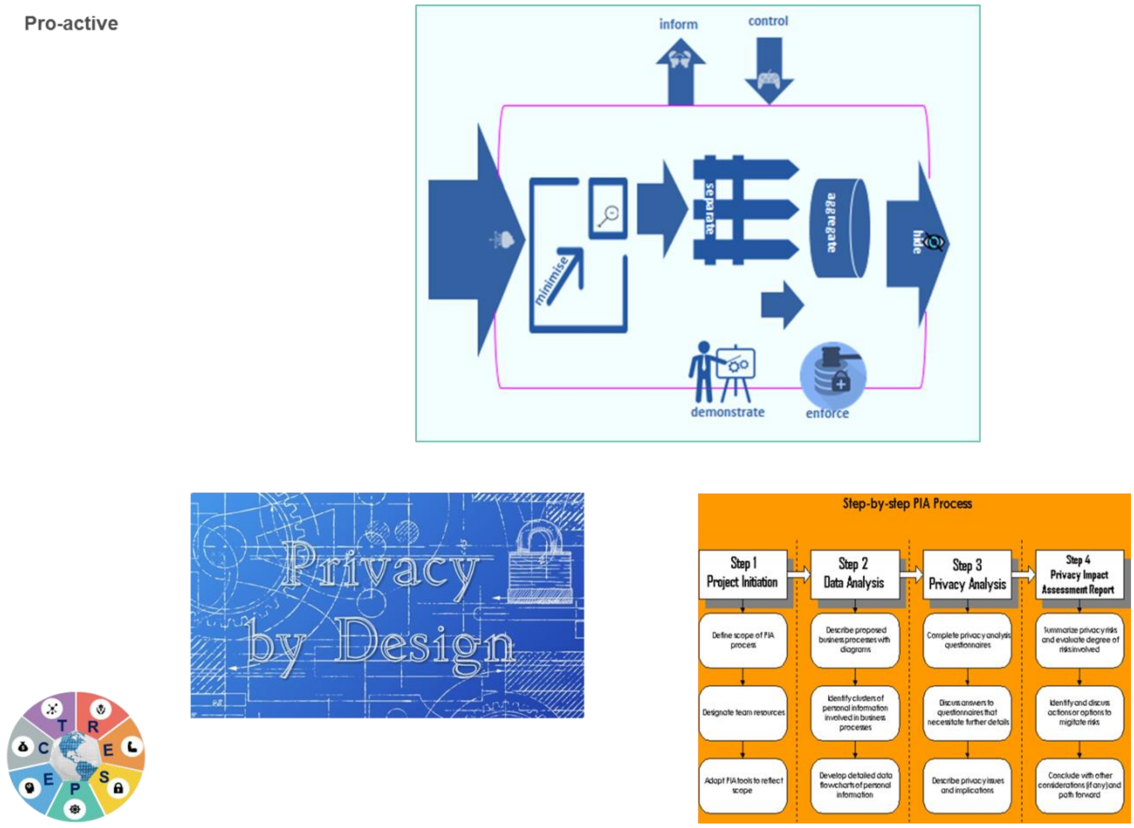

Pro-active
inform
control
minimise
separate
aggregate
hide
demonstrate
enforce
Privacy by Design
T
R
E
S
P
E
C
Step-by-step PIA Process
Step 1 Project Initiation
Step 2 Data Analysis
Step 3 Privacy Analysis
Step 4 Privacy Impact Assessment Report
Define scope of PIA process
Designate team resources
Adapt PIA tools to reflect scope
Describe proposed business processes with diagrams
Identify clusters of personal information involved in business processes
Develop detailed data flowcharts of personal information
Complete privacy analysis questionnaires
Discuss answers to questionnaires that necessitate further details
Describe privacy issues and implications
Summarize privacy risks and evaluate degree of risks involved
Identify and discuss actions or options to migitate risks
Conclude with other considerations (if any) and path forward

Figure 5: The privacy by design scheme and an overview of a PIA flow chart

Ethical

Why

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.

What

An organisation should be aware of the potential ethically 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, especially since it will be very hard to demonstrate the unintended appearance of these consequences.

How

Respecting the privacy of citizens and consumers and willingness to demonstrate transparency in the actions contribute to the creation of trust. We translate this into the following two conditions, namely (i) fair treatment of consumers and (ii) fair practices:

1. a fair treatment of individuals as citizens or consumers means a treatment where the privacy of individuals is safeguarded, where the autonomy of individuals is respected and where there is a prevention against unlawful discrimination and unfair exclusion.
2. fair practice means : (i) organisations are clear about their intentions and their practice, (ii) organisations show willingness to take responsibility and liability of their action and (iii) individuals have the ability to adjust their own role/position in a transaction.

These conditions means:

1. *Non-discrimination and stigmatization*. Personal data which are, by nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the

fundamental rights and freedoms. Sensitive personal data include personal data revealing racial or ethnic origin.[3] Other categories of sensitive personal data are data revealing political, religious of philosophical opinions and beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a person, data concerning health or data concerning a person's sexual orientation, medical and genetic conditions. Moreover, profile based actions can lead to stigmatization and confirmation of stereotypes in commercial domain and the public debate.

2. *Exclusion*. Using technology may exclude someone from receiving a service because of non-traditional analytics predictors such as a person's zip code, relationship status, or even social media use. Organisations need to be careful to ensure that their services are not excluding a group of people based on characteristics that are protected under equal opportunity laws or that are unwanted and that may negatively fire back on an organisation's reputation.

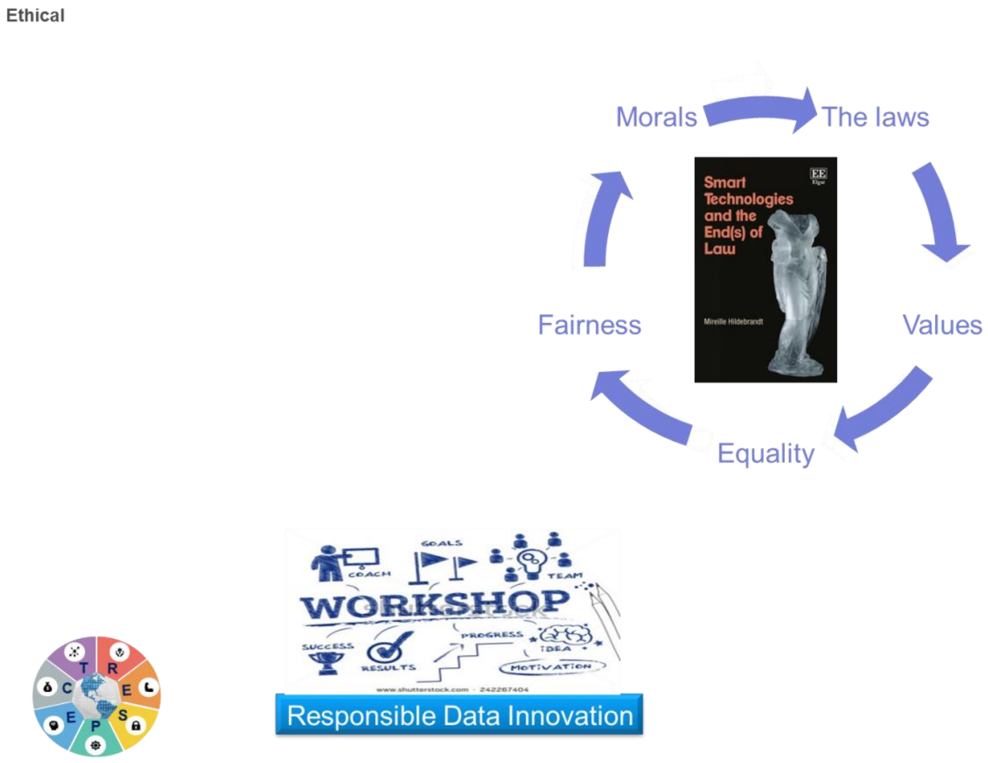


Figure 6: Ethical issues related to technological developments

[3] The use of the term "racial origin" in our label does not imply an acceptance by us of theories which attempt to determine the existence of separate human races.

Costs and benefits

Why

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 service offers 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.

What

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. These hard to deny difficulties determine much of the discourse on the costs and benefits of privacy.

We can add however, some substance to this discourse. Instruments that help understanding organisational costs are of help. This relates both to implementation costs (for instance installing a separate data protection officer in the organisation, or developing and implementing an organisational chain of responsibilities) and operational costs (having roles and responsibilities that need to be fulfilled).

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 are increased trust by clients and a potentially larger client base given positive reputation impacts.

How

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

Cost benefits

Sometimes it makes sense to look only at costs. This can be relevant when it is prerequisite to understand costs elements and the cost flows to several roles in the value web. But in many cases, it is short-sighted to only look at costs while leaving benefits aside. We assume privacy not only being a cost-incurring business value but having potential business benefits as well.

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 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". We can use several methods, 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 innovation, 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 organisation 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.

Cost-benefit

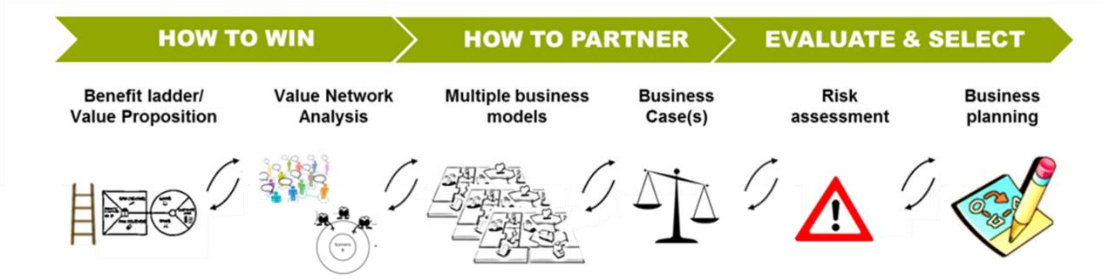


Figure 7: Instruments to assess costs and benefits of responsible data processing

Transparent

Why

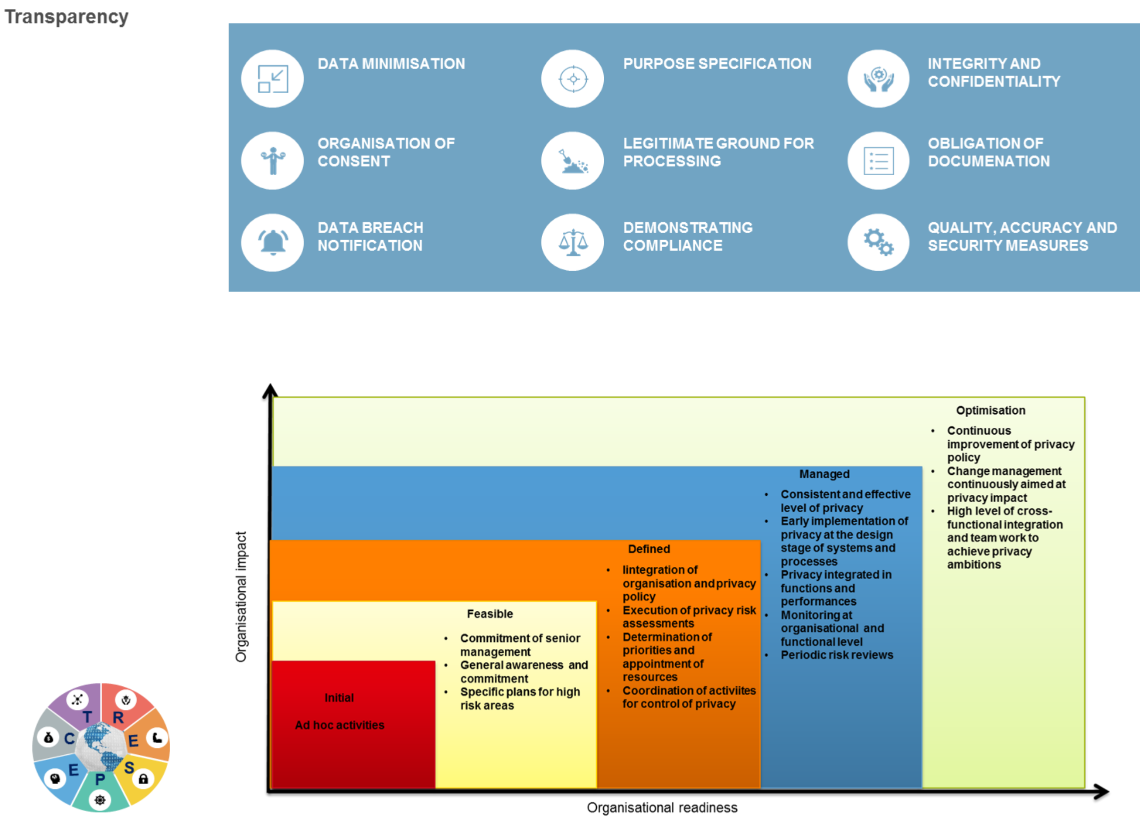
Restoring the present imbalance in which individuals become increasingly transparent to organisations while organisations are rather opaque to individuals means introducing transparency within the organisation. Many other domains already have organised transparency measures in order to meet societal 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.

What

Legal obligations (in the GDPR for instance) 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 responsibilities within the organisation improves transparency towards data subjects and employees. Behaving transparent creates organisations that act predictably, that behave trustworthy and that further a trusted relation with their clients.

How

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 should promote a responsible and mature attitude within the organisation with respect to the responsible processing of personal data as well. Other instruments that can be used are the adoption of certification schemes that indicate formal procedures the organisation will meet (and that will be audited) and adopting a code of conduct (which should be organised by a branch rather than by single organisations). Other instruments could be the establishment of a client panel that is used to discuss novel products or services and that may help in receiving feedback on the privacy maturity of the organisation. Benchmarking the organisation (for instance by using a privacy maturity model) could be a way to promote both internally and externally how the organisation performs in a responsible processing of personal data. Inserting a privacy section in the Annual report or creating an Annual Privacy Report are other means. Many of these instruments are part of behaving responsibly as well.



DATA MINIMISATION

PURPOSE SPECIFICATION

INTEGRITY AND CONFIDENTIALITY

ORGANISATION OF CONSENT

LEGITIMATE GROUND FOR PROCESSING

OBLIGATION OF DOCUMENATION

DATA BREACH NOTIFICATION

DEMONSTRATING COMPLIANCE

QUALITY, ACCURACY AND SECURITY MEASURES

Initial

Ad hoc activities

Feasible

- Commitment of senior management
- General awareness and commitment
- Specific plans for high risk areas

Defined

- Iintegration of organisation and privacy policy
- Execution of privacy risk assessments
- Determination of priorities and appointment of resources
- Coordination of activiites for control of privacy

Managed

- Consistent and effective level of privacy
- Early implementation of privacy at the design stage of systems and processes
- Privacy integrated in functions and performances
- Monitoring at organisational and functional level
- Periodic risk reviews

Optimisation

- Continuous improvement of privacy policy
- Change management continuously aimed at privacy impact
- High level of cross-functional integration and team work to achieve privacy ambitions

Figure 8: Instruments to promote transparency

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 not 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. 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 digitlal privacy and identities with an aim at contribution to proper societal solutions. The three institutes house 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. …

Disclaimer:

This report will be used to produce a formal TNO White paper on RESPECT4U. Please, cite this report as:

Marc van Lieshout, Somayeh Djafari, Petra Vermeulen (2017). *RESPECT4U*. TNO-report. The Hague: TNO/PI.lab.

April 3, 2017, The Hague

PI.lab website: https://www.pilab.nl/

Correspondence : marc.vanlieshout@tno.nl; +31(0)6-51246618