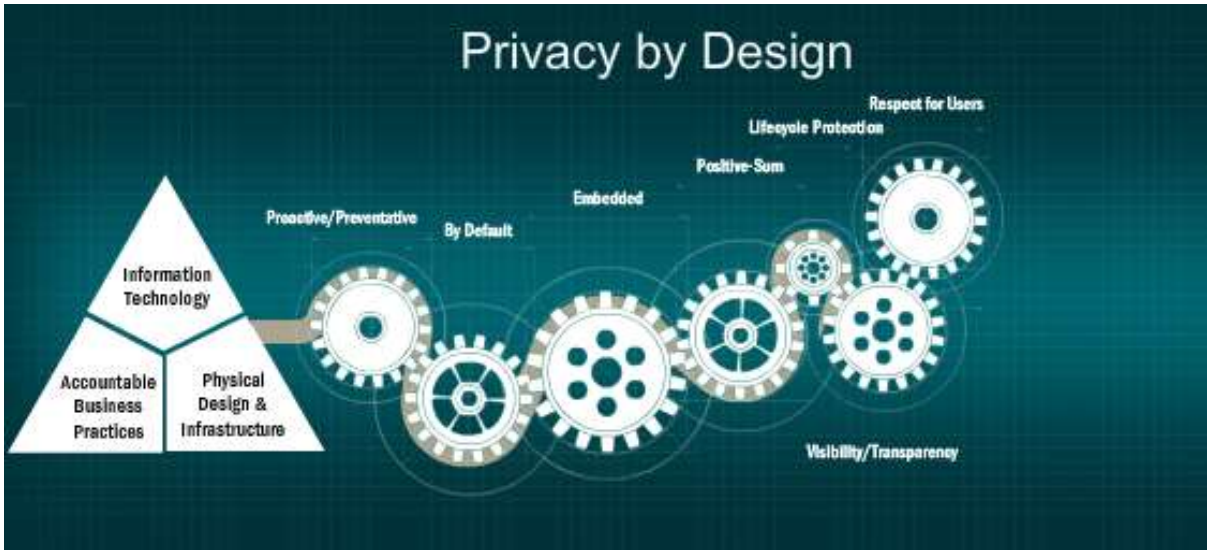
Privacy by Design and Smart Mobility

Wouter van Haaften
DUTCH ROUND TABLE FOR SMART MOBILITY LEGAL ASPECTS
RONDETAFELS.DITCM.EU

Beter Benutten AutomotiveNL DITCM Innovations Connekt Connecting Mobility

Privacy by Design and Smart Mobility

Based on the new European General Regulation Data Protection (GDPR), applicable as of May 2018, 'Privacy by Design'' must be employed in all applications in which personal data are being processed. This means that the in the design of the IT systems, in the business processes and the design of the organization Privacy by Design will be the standard for design and development of applications processing personal data. The considerations on Privacy by Design should start as soon as the outlines of a (Smart Mobility) service emerge, and preferably before the first steps in the design process have been taken.



Introduction

This aid is not a blue print on how to deal with personal data within Smart Mobility projects. The aid offers, by means of a systematic approach and examples, insight in the legal framework around the protection of personal data. It illustrates the necessity to apply Privacy by Design on all data protection sensitive services. Privacy by Design is a design approach and not so much a concrete practice or technology. A company, an organisation or a project team employs Privacy by Design when data protection is incorporated in the earliest designs of the service and when this attention is being maintained throughout the entire life cycle of the service. This method combines both technology and the way the organisation of the service provider is being designed.

Privacy by design should be applied when:

1. Deciding on the necessary (personal) data set;
2. Functionally designing the service;
3. Designing the information architecture;
4. Designing the IT;
5. Designing the organisation;
6. Designing the legal context and possible cooperation.

In short, when a Smart Mobility service that may involve personal data is developed the first question to put will be: are personal data well protected?

Personal data is all information related to an identified or identifiable natural person. Name, address of a person for instance are direct identifiers while a licence plate number or a MAC address of an on board unit are indirect identifiers. Since Smart Mobility services often process location data of the customer, and this data is being regarded sensitive, Smart Mobility services often will process sensitive personal data.

Goal

The goal of this aid is to create insight within the target group in the legal data protection aspects of Smart Mobility applications specifically in case of collecting and processing location data. Furthermore this aids attempts to implement data protection as a basic notion of functional design, technical design and of the organisation of Smart Mobility solutions in such a way that design and development choices can be explicitly judged on compliance with the GDPR. The employment of Privacy by Design will, next to the protection of the privacy of an individual, also support the data security. This will lead to less data protection risks during operation, such as abuse or unlawful use, loss or mutilation of personal data.

Target group

The target group for this aid primarily are the service providers, since they will have the legal role of controller in most cases. They will design the processes in which Privacy by Design will be employed on behalf of their customers. Other target groups are those involved in the system- and organization design processes in other ways, like OEM's, principals, consultants, data- software- and hardware providers, both large or small, experienced or start-up.

Controller

The controller plays a central role in the data protection legislation. It is the one to decide upon the purpose and means of the processing of personal data and/or the one who has a dominant position for instance within a consortium or a data chain. In case that an initiative or assignment for a Smart Mobility project has been defined in general terms, usually the contractor will be the controller because he will in translate the functional specifications into the more concrete purpose and means of the processing. Projects initiated by the public authorities should demand that the services comply with the principles of Privacy by Design.

Privacy by Design; 7 design notions

A recognized approach to get to Privacy by Design is the framework developed by Ann Cavoukian, the former Information and Privacy Commissioner of the Canadian province of Ontario. The framework introduces seven design notions:

1. **Proactive** not Reactive; **Preventative** not Remedial
2. Privacy as the **Default Setting**
3. Privacy **Embedded** into Design
4. Full Functionality — **Positive-Sum**, not Zero-Sum
5. End-to-End Security — **Full Lifecycle Protection**
6. **Visibility** and **Transparency —** Keep it **Open**
7. **Respect** for User Privacy — Keep it **User-Centric**

1. Proactive not Reactive; Preventative not Remedial

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

A provides a Smart Mobility-service in the car of B. Therefor data from that car are sent to the back-office. The licence plate number is one of the data. After identification the licence plate number has lost its value in the process. The system has been designed in such a way that the licence plate number is deleted just after identification and before further processing.

2. Privacy as the Default Setting

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

The data B provided, still personal data, are being processed by A with B's consent. The processing system has arranged by default how long the personal data can be stored, who has access to the data and what processing is allowed under B's consent.

3. Privacy Embedded into Design

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

Apart from deciding on the purpose and the means of the processing and the compliance with the data protection law A makes sure that B's data are properly secured. Therefor authorisation and authentication technology is used, and data will be encrypted if necessary. When setting up the administrative processes A makes sure that unauthorised persons can have no access to B's personal data.

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

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

The interests of both A and B have been articulated clearly beforehand and have been communicated accordingly. Based on this practice B trusts the service A provides as well as the security of that service and therefor is willing to share his personal data, knowing that A will comply with data protection regulations.

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

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

A makes sure that B's personal data can not get into unauthorised hands. Therefor he takes both technical, logistical and organisational measures throughout the data chain. On top the end of the chain is clearly marked by deleting the personal data that are no longer necessary for providing the service.

6. Visibility and Transparency - Keep it Open

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

Along with transparency about his interests A also is transparent about how he processes B's personal data by means of a data protection declaration. This declaration shows how the confidentiality of the data within the processes has been guaranteed. The declaration contains information on, for instance, the organisation and security measures that have been taken.

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

Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong

privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

In his communication the starting point of service provider A is the position of customer B. He is clear about how he complies with legal requirements and what his business model is, in order to make clear what the data are being used for, including the possible sales of data.

Instruments

In order to implement Privacy by Design in Smart Mobility both standardisation and monitoring of the application of Privacy by Design will be required. Within the new GDPR also a stronger accent has been laid upon monitoring and enforcement of the rules, for instance with high fines. The tendency to get from 'tell me' to 'prove it to me' supports the development of Privacy by Design because it leads to more transparent systems and processes. In this paragraph a few instruments are brought up that may help while establishing Privacy by Design.

Privacy Officer

The privacy officer is being appointed at board level as an independent judge of the state of data protection within an organisation. He sees to the compliance with data protection regulations either within one organisation, within a consortium or even at Trade Association level. Within the Smart Mobility community all three variants are possible. De privacy officer can, because of his independence, expose potential non-compliance with the data protection rules and facilitate the board to take action. In this way non-compliance can be avoided in many cases.

Privacy Enhancing Technologies

The core of Privacy by Design consists of Privacy-Enhancing Technologies (PETs): technical measures aimed at the protection of the privacy of the subjects and leading to an ‘end-to-end’ security, identity- en access management and to a strong -function based- authentication. The opportunities to monitor via logging and auditing of the operation will achieve that subjects can trust the system not to collect, process, store and spread their data unlawfully. Meanwhile the controller will supply the necessary organisational measures like role separation and physical access security.

Multi-Actor-Analysis

A Multi-Actor Analysis contributes to transparency with all actors of all interests to be detected in advance and to be recognised by all stakeholders. Thus the analysis helps creating sufficient support from the stakeholders.

Privacy Impact Assessment

A privacy impact assessment (PIA) is a good method to get an overview of all threats and risks occurring while processing personal data. Based on the results of the PIA it can be decided which type of Privacy by Design will be required. Consequently this will lead to a functional design in which the various functions required are described in a coherent way.

Monitoring

Above all compliance with the privacy demands will have to be monitored. To this purpose however frameworks are yet to be developed. http://privacypatterns.org could serve as an example as to what templates could be chosen.

Annex: New Legislation

General Data Protection Regulation (EU) 2016/679

In the GDPR Privacy by Design has been explicitly adopted in Article 25. The regulation has entered into force on 25 May 2016 and shall apply from 25 May 2018. It seems wise to hold on to the new regulation particularly when the service will be in business after the application date.

Article 25
Data protection by design and by default:

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data that are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Article 42
Certification

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance

with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organizations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

3. The certification shall be voluntary and available via a process that is transparent.

4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

6. The controller or processor which submits its processing to the certification mechanism shall provide the certifi cation body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in

Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.

8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.