Privacy by Design

www.tuvopensky.com

OPENSKY
A TÜV Rheinland Company

Introduction

Back in the mid-90s, the former Canadian Information and Privacy Officer (Ontario), Ann Cavoukian, developed what has been called the Privacy by Design ("PbD") Framework. The aim was to derive a set of proactive privacy considerations out of the existing common data protection ("DP") foundations laid down among others in the Generally Accepted Privacy Principles ("GAPP"), the OECD Guidelines on the Protection of Privacy (1980), the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108, 1981) and various national DP laws and regulations.

The original framework comprised 7 core principles:

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

These principles represented the efficient implementation of privacy requirements and their processes within organizations. Over the years, this framework has influenced many DP laws worldwide and even was partially adopted into laws, for example into the German Telecommunications law TDDSG back in 1997.

A solid concept endures. As we can see by the renaissance of PbD in the EU General Data Protection Regulation ("EU GDPR"), which stipulates the requirement of implementing PbD in Article 25, the approach is more applicable today than ever. The EU GDPR is also applicable to companies outside the EU if they are targeting EU customers and markets (market principle). This brings global attention to the requirement of PbD, and its positive side effects as described further in this article. Besides this, PbD is on its triumphal march through various international data protection jurisdictions.

Criticism of the concept of PbD often states that it is too vague when it comes to its application and implementation in technical environments, and that it is challenging to implement. Compared to common ISO Standards like the 27000 family, there are no specific measures and/or control structures to be followed.

To counteract this, we've found that it's important to assign responsibility for PbD to the correct people, train them in the concept and their role in its implementation, and ensure they keep informed of the latest news and changes involved in its application. In this whitepaper we will emphasize the customer value realized by proper implementation of PbD as a comprehensive concept using our experience in past implementations for various international customers.

Perspectives

At the outset of every PbD implementation project, the question is raised "where do we start?". One place to start is the applicable data protection law. The EU GDPR legislation for example on the one hand details the technical perspective but does not elaborate on the organizational side when it comes to PbD. Article 25 is titled "Data protection by design and by default". Section 1 states that 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".

Implementing companies must analyze both technical and organizational measures and balance these against the risk associated with a specific type of processing. Risk is a key concept in the EU GDPR. In fact, Article 25 indicates that "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" must be taken into account when implementing PbD. The regulation ensures that the protection of individuals' rights and freedoms are of the utmost concern.

For PbD technical measures, it seems obvious to make use of appropriate encryption, anonymization and pseudonymization technologies, especially in Big Data projects. It becomes a little bit more complicated if the risk of de-anonymization exists, including the ability to identify the personal data based on the context of the data. It has been estimated that in many situations it could take as little as 4 queries to get 70% of data correctly de-anonymized. As an example, if your HR department is going to perform a salary comparison based on anonymous data (no names, no dates of birth), the risk to identify the natural person behind "John Doe" increases with the amount of additional information (e.g. type of college degree) and the size of the group (e.g. he's in a department with 3 employees).

Depending on the size of the organization, hierarchical structures, and reporting lines, the assumption could be made that naming a data protection officer (DPO) who is responsible for PbD should sufficiently cover this requirement. It certainly does not. This responsibility is shared by many people and spread out across many parts of the organization. If we go back to Article 25 Section 1, we must consider the point in time when DP comes into play ("… at the time of the determination of the means for processing…"). Therefore, responsibility for PbD is in force at the earliest possible point in time, for example:

- As part of the request/demand process (especially cloud)
- For IT projects in the planning phase
- In the staffing of central committees like the enterprise architecture and/or information security committee

The positive side effect of implementing PbD early on is that companies can avoid delays or showstoppers that could arise when DP requirements are reviewed belatedly, for example after contract signing with an external supplier or as a project goes live tomorrow. In these and other scenarios, it becomes painfully obvious that a subsequent change in implementation, configuration or structure could lead to a massive cost and resource impact.

Privacy by Design as an Innovative Approach

Instead of embracing the PbD requirement as another legal obstacle for IT to hurdle, it is a smart move to welcome it as a chance to fulfill multiple legal and regulatory requirements. Early recognition of privacy requirements in the form of implementation of adequate technical and organizational measures can sufficiently cover the requirements of IFRS, due diligence as a stock listed company (e.g. during supplier selection), ISO27001 (A.14.1.1, A.18.1), IP Law, EU Trade Secrets Directive and many other regulations and frameworks. By combining different legal requirements and pointing out the overlapping areas of implementation and adoption, an innovative privacy approach could emerge. This approach of innovative standardization and harmonization of the set of measures and activities in the technical and organizational implementation is invaluable in saving time and resources. It no longer leaves room for isolation and siloed work within the information security and privacy functions of companies. Many of the huge information security tool providers have written add-ons to their offerings to extend a company's existing tool platform to include privacy functionality.

Privacy is on the rise to become more and more a quality gate that is capable of challenging products, services and the organizations themselves to evolve in a future proof, reliable and secure way. The most positive outcome of this innovative privacy approach is that it spreads its value in many directions. Customers can now trust that business, authorities and enforcement ensure that all legal and regulatory requirements are met, and the company is limiting its risk of liability and potential fines. A mature implementation of PbD, regularly reviewed and certificated, disciplines the stakeholders to follow defined paths and raise their level of overall security.

Creating Value

The decision level of an organization usually asks first, "what will be the costs?" and "what is in it for me?". From our customers' experiences, implementing privacy by design is often more of a "connect the dots" game rather that a greenfield approach.

Most companies have a defined process for areas requiring privacy by design. For example, to add PbD to software development efforts, a review loop regarding the purpose of processing and the data to be processed can be added in. Often this review loop can be beneficially extended by adding approvals required by other internal and external obligations, such as (US) ITAR/EAR or the companies' information security policies (classification of data, region of processing). When it comes to the organizational perspective, relevant formats are already established; you now must ensure that the data protection persons responsible are invited to the appropriate council or steering committee. To identify the dots (synergies) and to connect them, it is often helpful to get an outside expert's view.

We chose two examples below of successful additional value creation from our practice for our customers.

The Big Data Project

One of our SMB industry customers in Eastern Europe was planning a big data project to analyze certain information out of their Operational Technology (OT) environment in real-time. Individual user IDs tagged the transactions and adjustments within the source systems. Each system also had a small HR mini master dataset to allow for processing machine-related personnel data for resource scheduling purposes. The target system was located in the cloud ecosystem of a US supplier. The customer was located within the EU; European data protection laws therefore were applicable.

THE PROBLEM

The Controller (responsible party for the processing of personal data) had gathered the original data for granting access to the OT systems and to ensure stable operations. The data usage for another purpose (analytics in the cloud) was not foreseen or transparent to the data subject and, because this was another (additional) purpose for use, there needed to be legitimate grounds for its use. Due to the lack of legal necessity for the processing, the only option for legitimate use seemed to be a written declaration of consent from the affected data subjects: 1400 employees. This was a formidable, unrealistic task. Furthermore, legitimate processing of personal data by the US cloud provider (the processor) required adequate contractual stipulations, but the processor was only willing to provide a nonnegotiable standard contract. Another roadblock.

THE SOLUTION

After a deep dive into the desired outcomes of the analysis and weighting of the value that the personal data might add to the analysis, it became apparent that the specific personal data wasn't mandatory for personnel planning purposes. To avoid the contract discussion, the best solutions was to anonymize the data at the source systems, to ensure that there would be no transfer of personal data outside the EU. This was accomplished by the installation of a lean software agent on every source system that anonymized the data transferred to the target system. The implemented algorithm also ensured that the risk of contextualization (de-anonymization by surrounding non-personal data) could be minimized to an acceptable level. This solution illustrates the implementation of privacy by design – the design of the software to anonymize the data – and privacy by default – the automatic default operation of the software on every source system.

The Medical Project

A large international company was planning to move its centralized expatriate database (HR data, vaccination history, company medical officer reports, etc.) to a global shared service in India. The central IT department did a great job; they issued an RFP, completed a detailed requirements review with the top provider and even flew to India for an onsite meeting with the shortlisted company. After a two-month proof of concept phase, the contract had been signed. Before migrating the involved databases, the project lead thought it might be a good idea to inform the data protection officer.

THE PROBLEM

Employee data from various countries with individual data protection laws and regulations, and therefore different legitimate grounds for the specific processing in a centralized database, was being transferred to an unsecure third country. The DPO was brought into the project after the contracts were signed, and he was therefore unable to negotiate DP relevant elements such as migration setup, encryption and deletion, and subcontractor involvement. Furthermore, it could not be ensured that the planned processing was fully compliant with all applicable data protection laws.

THE SOLUTION

The contract had to be put on hold. The DPO and legal department jointly drafted an amendment covering the DP elements that needed to be agreed upon with the provider. Management identified the risk due to a lack of proper implementation of privacy by design in its IT purchasing processes and provided the DPO with an approval process in the demand phase of IT purchasing for future initiatives to ensure early DPO involvement. Company stakeholders performed further problem analysis, gathered the DP requirements of every involved company, and developed a set of structured data protection requirements to be included in all RFP documents for future projects. A set of contractual templates was also generated for future projects. This solution illustrates the importance of designing privacy into projects, even at the contract stage.

SEPTEMBER 2018

TUV Rheinland OpenSky
295 Foster Street #100
Littleton, MA 01460
1-888-743-4652
info@tuvopensky.com

www.tuvopensky.com

OPENSKY
A TÜV Rheinland Company