Privacy by Design

as license to operate for new business initiatives

Privacy by Design as a key driver for effective, efficient, and high-quality new business initiatives. In this rapidly changing digital landscape, it is essential to shorten the time to market for your new business initiatives to ensure you keep a competitive advantage. At the same time, it is key to keep and improve the trust relationship with your customers. To do this successfully, a sustainable business strategy that aligns with todays and tomorrow's challenges and customer expectations is needed. Key to that strategy is embedding cybersecurity and privacy within your organisation to ensure your customer's personal data is protected. This will create a unique selling point for your new product, service or other business initiative and positively influence your position in the market. Implementing Privacy by Design is the answer to effectively and efficiently benefit from all these advantages.

1 A powerful tool with digital trust as an outcome

To understand what competitive advantages Privacy by Design can provide, we first need to understand what it entails exactly and how competitive advantages may be created. Data Protection by Design and Default (commonly referred to as Privacy by Design) is not just an important requirement from the GDPR. It is a way of working that creates a lot of possibilities when applied correctly. It provides guidance for important decision-making moments by embedding data protection in the lifecycle management of your products and services. It creates quality and trust for your customers with regards to data protection. In short, it provides your organisation the approach and tools to proactively embed data protection measures to ensure effective data protection, while being cost efficient.

How can you achieve this end state? The answer is ‘shift-left’ as much as possible in your development process. Shift-left is thinking about risks, including data protection risks, as early in the process as possible when the cost of compliance is lower compared to doing it later in the process when trying to bold data protection onto something already developed and launched. Shift-left means that your customers’ personal data is protected from the start of the development process. It also means that you can avoid iterations at a later stage which cause delays in the time to market and costly changes, because the requirements and risks have been considered and implemented at an early stage.

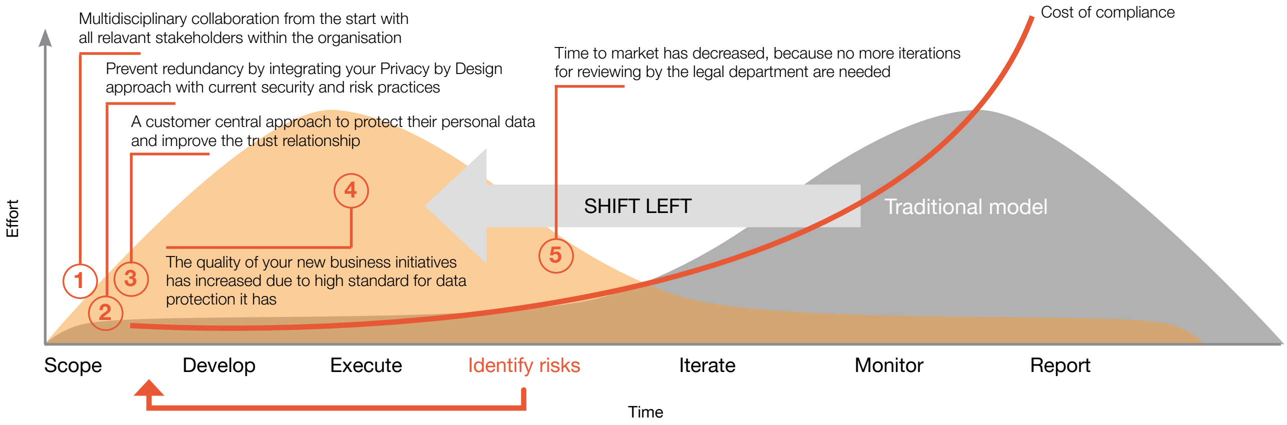

Multidisciplinary collaboration from the start with all relavant stakeholders within the organisation
Prevent redundancy by integrating your Privacy by Design approach with current security and risk practices
A customer central approach to protect their personal data and improve the trust relationship
The quality of your new business initiatives has increased due to high standard for data protection it has
Time to market has decreased, because no more iterations for reviewing by the legal department are needed
Cost of compliance
SHIFT LEFT
Traditional model
1
2
3
4
5
Effort
Scope
Develop
Execute
Identify risks
Iterate
Monitor
Report
Time

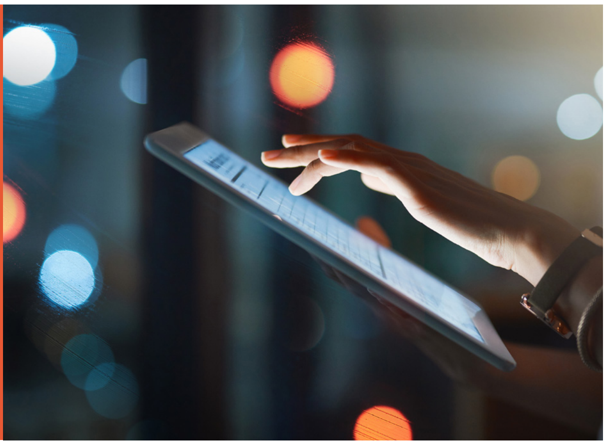
Figure 1: example of the benefits of a ‘shift-left’ by applying privacy by design

2 Embed Privacy by Design in your existing practices

Privacy by Design is not a stand-alone practice. Privacy by Design should be part of your existing risk and security practices for your business initiatives. This means two things. First, Privacy by Design can be part of existing risk assessments and may help identify mitigating data protection measures in line with other risk mitigating effort, thus preventing duplication. Second, the foundation of your current security practices for new business initiatives can also serve as a foundation for your Privacy by Design approach. For example, at the moment data is collected as part of the existing logging and monitoring capability, noise can be added which protects the data subject involved. Adding this in a later stage will leave this risk unaddressed for a longer period, which can ultimately make it impossible to repurpose the data for analytics without risks to the data subject.

To give you an idea of how the implementation of Privacy by Design can look like, we will use an example case that shows the implementation and the added value and advantages.

Clouddrive X is a fictive cloud service provider and an agile organisation. They are planning on building a new application. This application provides an online service for secure omnichannel communication, including file sharing, with the clients' end-client. With this application Clouddrive X can enable their clients with a privacy and security friendly application to ensure their end-users personal data is processed safe and correctly.



In Clouddrive X, roles and responsibilities have been defined regarding new business initiatives. The product owner is responsible to deliver client value with the new application. He needs to make sure he will gather all input from diverse stakeholders. In most cases, stakeholders with a focus on value protection such as privacy and security experts are not part of this iterative consultation or are only involved at a later stage. However, at Clouddrive X it is custom to involve privacy and security experts from the start of projects as the delivery and protection of value are both within the remit of the product owner. Another advantage is that their existing security risk assessments can easily incorporate privacy risks and mitigating measures. There is no need to reinvent the wheel or to develop a completely new practice for privacy purposes.

These stakeholders ensure that the information security & privacy requirements are known and recognised by the product owner so that the product team can implement them. The inclusion of these stakeholders at an early stage ensures the data protection related requirements are taken into account during the development, not afterwards. This inclusion leads to the result that the problem-solving expertise of the project team is now combined with the subject matter expertise of their cyber and privacy colleagues. It also enables proper weighing of potential trade-offs since all departments that need to play a role in this new initiative are involved at an early stage with their respective roles and responsibilities.

The requirements for privacy are now defined in the development phase of the initiative.

This creates the possibility to make the requirements more understandable for a larger group of people and more actionable. Based on best practices derived from other projects, the project team adheres to the requirement of data minimisation by using a standardised anonymisation solution which is provided as a central capability. This allows the new application to analyse the personal data without compromising the data subjects and results in valuable statistical insights. This same data is also used to detect fraud or other malicious threats to the tool.

The team has bi-weekly meetings to discuss progress and approach. All defined requirements are also discussed together with new functionalities and features.

The team has considered privacy requirements at an early stage and thus 'shift left' has taken place. Privacy is addressed throughout the entire lifecycle of the application. All new functionalities and features take the requirements into consideration before they are developed. This new view creates the possibility to have valuable insights related to the processing of the personal data and possible risks are addressed at the right time.

Normally, the team would have the legal department and the privacy department look at the finished application. Because Clouddrive X has implemented Privacy by Design fully, this is no longer the case.

The time to market has now decreased by more than 3 months. Before implementing Privacy by Design, the legal departments would review at the end after additional iterations were required. Going back and forth between Legal and Security to sufficiently mitigate the risk is a time-consuming process. This process has now become more efficient and much more effective. A functionality or feature of the application is developed while taking the requirements for value protection into consideration. Doing so ensures that the data protection requirements are met.

Repeating the privacy by design lifecycle leads to business and development teams with growing expertise in PbD. As a result, they are able to apply PbD principles more independently by themselves. As their efficacy increases, the required constant input from security and privacy colleagues decreases, leading to an efficient division of the workload.

The application now shows more quality each delivery without rework to bolt on data protection requirements. Implementing Privacy by Design has made all this possible.

In the future, Clouddrive X will have self-sufficient development teams that are able to implement privacy by design by themselves.

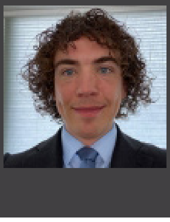
3 How can I enable competitive advantage whilst keeping and improving my customers' trust?

Our practice touches on all aspects of your operating model. You have to align why you are doing Privacy by Design to your strategy. When adjusting the governance, you need to ensure the people have the proper processes and tools to deliver on their responsibilities. We can support you with multiple aspects of the matter. Together we can build a sustainable Privacy by Design program that will fit your organisation and current way of working. We have all the business, user, technical and legal knowledge to support your organisation in evolving to the next level of data protection maturity and a track record that supports this.

Would you like to discuss the matter more in depth, or would you like to discuss any aspect a bit further, feel free to reach out. We would be happy to clarify.

Contact:

Bram van Tiel
Partner Cybersecurity &
Dataprivacy, PwC Netherlands
Tel: +31 (0)62 243 29 62
e-mail: bram.van.tiel@pwc.com



Job van Ommen
Senior Manager, PwC Netherlands
Tel: +31 (0)64 201 78 55
e-mail: job.van.ommen@pwc.com

© 2021 PricewaterhouseCoopers B.V. (KvK 34180289). All rights reserved.
The information transmitted is intended only for the person or entity to which IT is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from any computer.