GDPR series: A design for life? Designing the future of privacy

Nicola Flannery, Deloitte Risk Advisory Ireland, discusses the Privacy by Design requirement under Article 25 of the General Data Protection Regulation and outlines some practical steps that organisations can begin to implement now

In an era where 'big data', 'innovation' and 'individualised offerings' are the norm, organisations are empowered to use consumer personal data to constantly find new ways to create commercial opportunities, 'quick wins' and operational efficiencies, all with the aim of driving revenues or enterprise value.

However, pushing innovative boundaries in this data-driven world increases privacy risks, and data breaches are beginning to be the norm. Consumers are also feeling the need to have more control over their data and legislators are driving privacy legislation with a heavy emphasis on the rights of the individual.

This ever-changing regulatory landscape can be frustrating and feel quite stifling for innovation-conscious organisations. Striking a happy balance can seem very difficult, and more often than not, organisations view privacy risks as part and parcel of business operations, instead of really considering what can be and needs to be done to eliminate these risks and safeguard their consumers' personal data. Gaining consumer trust also builds brand and reputation.

So what's the magic potion? Where does an organisation even start?

And how can Privacy by Design help?

Privacy by Design background

Privacy by Design ('PbD') has actually been around since the 1990s when it was coined by then Information and Privacy Commissioner of Ontario, Canada, Dr Ann Cavoukian. Since then, it has been adopted as a fundamental privacy concept by Data Protection Authorities around the world.

Despite not being a new concept, PbD does have an air of mystery about it that has resulted in resistance from organisations not fully understanding how to incorporate it into everyday business. However, the new European General Data Protection Regulation ('GDPR') has now codified PbD and Privacy by Default under Article 25, and with little formal guidance on how to implement these concepts — and the deadline of 25th May 2018 looming — organisations now need to grab them with both hands and get to grips with them.

What is it?

PbD simply means building privacy into the design, operation and management of any given IT system, project, software development, design specification, business practice or operation that collects, processes and retains personal data. Privacy by Default stipulates that an organisation's modus operandi should be to automatically apply the strictest privacy settings to any new product or service. In other words, a consumer should not have to adjust any privacy settings; they must automatically be set to the most private.

The two concepts operate on the basis of privacy concerns being addressed proactively instead of reactively. Too often, organisations deal with privacy concerns and even breaches when and if they arise in an ad hoc manner. Although in some cases, this may be effective in mitigating the risks that have arisen, more often than not this approach leaves organisations open to substantial risk and considerable brand and reputation damage — and that's before you factor in any financial damage resulting from not having the correct privacy controls in place to prevent the concern or breach in the first instance.

PbD and Privacy by Default aim to prevent these risks from arising, and ultimately to avoid the damage which could result in the organisation losing its competitive edge.

Why?

PbD and Privacy by Default envisage a future whereby privacy assurance is embedded into day-to-day operations, forming a significant part of an organisation's risk structure. This supports and underpins compliance with various regulatory frameworks and has benefits going beyond keeping the privacy regulators happy.

The greater customer trust and confidence that in theory results from ensuring the protection of customer personal data can mean a greater competitive advantage. What about operational benefits? Ensuring that privacy is embedded across the entire data lifecycle of any project will not only reduce the likelihood of a data breach, but will reduce the effort and cost that is spent on dealing with privacy concerns that frequently arise.

If organisations require an incentive beyond the requirement for PbD and Privacy by Default in the GDPR, they can look no further than the fines for non-compliance (2% of global annual turnover up to a maximum of 10 million euro or 4% of global annual turnover up to a maximum of 20 million euro). This should provide more than enough justification to invest time and resources now in implementing a PbD framework and controls.

Though we are currently awaiting further guidance from the regulators on the GDPR provisions including PbD, we do know that the GDPR encourages the use of codes of conduct. In Canada, where PbD was 'created', there are specific PbD certifications that organisations can obtain, and it is more than likely only a matter of time before the EU follows suit. Getting ahead of these developments would be a smart move.

> ***"In Canada, where PbD was 'created', there are specific PbD certifications that organisations can attain, and it is more than likely a matter of time before the EU follows suit. Getting ahead of these developments would be a smart move."***

How?

So with official guidance yet to be issued by regulators, what can organisations do now to begin developing their PbD framework?

Review the as-is: One of the first priorities is to identify and assess the lifecycle of personal data within your organisation. Establish data lifecycles that map out the flow of personal data from collection, manner of processing, storage and transfer, right through to retention and destruction. Use these maps to establish data inventory, categorising all the personal data with as much detail as possible, where it originated and who the 'data owner' is. Data owners within organisations who understand the privacy implications behind personal data are key to effectively managing those data.

Afterwards, organisations should consider how they currently approach new projects and at what point privacy requirements are taken into consideration.

Review the privacy policies and processes you already have in place. Is your privacy statement transparent enough and does it describe all personal data being collected and the purposes for the processing? Do you have the correct consent mechanisms for the collection of this data?

Privacy settings should be available for individuals to control how they want their data to be processed by an organisation, and there must be a means of access for individuals to view all data collected from them.

Consider also how your retention policy works. Ensuring that data owners across the organisation are managing personal data in line with the policy, and consulting information security when personal data need to be securely stored or securely destroyed, is key to keeping data inventories and data lifecycles clean, as well as adhering to data minimisation principles under the GDPR.

Leverage the existing or create a new privacy standard: The next thing to examine is current governance structures and the risk processes your organisation already has in place. Organisations should use their existing operational processes as a base from which to add on privacy considerations. If you are an organisation that processes personal data on a large-scale or processes sensitive personal data, then create your own PbD standard.

A policy should outline the standard and issue requirements across the organisation in terms of applicability, implementation and monitoring of ongoing compliance. Consider how you gain value from your customers being aware of your policy. This could help to raise trust in your organisation.

Data Protection Privacy Impact Assessments (DPIAs): DPIAs should form a key part of an organisation's PbD approach. Under Article 35 of the GDPR, DPIAs must be carried out on any new project that processes personal data that are likely to result in a high risk to the rights and freedoms of individuals.

The DPIA must include at the very least:

- a description of the processing operations;
- the purposes of the processing and an assessment of the necessity and proportionality of the processing; and
- an assessment as to the risks posed to the rights of individuals and any measures taken to mitigate these risks.

An organisation's Data Protection Officer ('DPO') must be involved and if the DPIA establishes that there is a high level of unmitigated risk, then the relevant supervisory authority must be consulted prior to any processing. A good approach to incorporating DPIAs into your PbD standard is to create a short form PIA which performs an initial privacy review at the beginning of any new project. This short form DPIA will then identify if a subsequent long form DPIA is necessary.

Involve your business and technology owners: PbD is not simply to be approached from an organisational and regulatory perspective, but entails a technical approach too which is often overlooked by organisations.

(Continued on page 8)

(Continued from page 7)

As data protection risks are ever-changing due to advancing technologies, so too are the privacy enhancing technologies that help mitigate these risks. Privacy Enhancing Technologies ('PETs') have been defined by Borking and Blarkom et. al (Handbook of Privacy and Privacy-Enhancing-Technologies (2003)) as 'a system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of functionality of the information system'.

Ensuring that your organisation assesses the level of risk it faces, versus the level of technological measures it needs to lower this risk, is key. PETs such as encryption and the use of metadata and access control lists are examples of technologies that can enhance and support PbD. However, the key to successful implementation of PETs involves engaging with your Chief Information Officer and information security and development teams as stakeholders, to bridge the gap between governance from a regulatory and organisational perspective and IT governance. Those conversations need to start now.

Look forward and commit: Once you have understood what PbD is and how it can become operational within the organisation, the work of establishing an implementation roadmap with support from key stakeholders can begin. This support often means investing in resources and/or privacy enhancing technologies and a solid commitment budget-wise. Being prepared, mobilising the right individuals and taking the first steps is half the battle.

Training and awareness: PbD can only be truly successful if it is embedded end-to-end within an organisation's business operations, from governance and accountability, right through to training and awareness. An organisation's employees must also embrace PbD as part of the privacy culture. Therefore regular training for all employees, with key risk training for data owners and teams who handle personal data on a daily basis, is a must.

Privacy by Design is here to stay, and so embracing rather than resisting the change and creating a proactive culture within your organisation will result in benefits that far outweigh the effort required to implement it.

Beginning now, and taking a three-pronged approach — looking at things from an organisational, technical and legal perspective — is key to identifying any gaps and preparing your organisation to be fully compliant with the GDPR by May 2018.

Nicola Flannery
Deloitte
niflannery@deloitte.ie