8 Hallmarks of effective Data Protection by Design and Default

Robert Maddox, International Counsel, and Stephanie Thomas, Associate, Debevoise & Plimpton LLP share key advice for ensuring data protection by design and default from the very outset

Whilst the EU and UK General Data Protection Regulation ('GDPR') requirements to implement 'data protection by design and default' are standalone obligations, they draw together, and build upon, the GDPR's core and binding data protection principles. This is true particularly in terms of the accountability principle and the data minimisation, purpose limitation, security and transparency requirements. Uniquely pervasive, data protection by design and default requires action before an organsiation has even collected personal data. It encompasses the entire lifecycle of a product or service that may ultimately involve processing personal data.

In common with much of the EU and UK GDPR, the obligation for data protection by design and default is intentionally non-prescriptive in order to remain technology neutral and facilitate evolution of implementing measures over time. It is defined open-endedly, limited only by express requirements to consider 'the state of the art, the cost of implementation and the nature, scope and context and purposes of processing'. This broad definition has afforded both organisations and Supervisory Authorities some latitude, but it has also brought uncertainty. Further, there is no direct parallel under the Data Protection Directive (95/46/EC), the EU GDPR's predecessor, on which to build.

Since the EU GDPR's entry into force five years ago, a clearer understanding of the relevant legal and regulatory expectations is emerging. This is influenced by recent guidance from, among others, the UK Information Commissioner's Office, coupled with insights from enforcement action —including the Irish Data Protection Commission's €265m penalty against Meta in 2022 for alleged EU GDPR failings, including under data protection by design and default.

Embedding data protection by design and default can be challenging and may require a culture shift and new ways of working. In this article, we distill actionable examples of how the requirement can be met in practice.

Hallmarks of Data Protection by Design and Default

There is no one-size-fits all approach to data protection by design and default. Nevertheless, hallmarks of an effective framework might include the following.

Engage early (do not be caught off guard): As stated above, data protection by design and default requires organisations to address data protection requirements prior to collecting personal data. The antithesis of 'data protection by design and default' is retrofitting compliance, which in some cases, may never be possible.

Through early engagement, organisations can help to ensure that they are developing products or services that will comply with data protection requirements rather than pursuing commercially desirable, but ultimately non-compliant offerings. The latter, often identified only later in the development lifecycle, could lead to significant sunk costs, or worse, enforcement and litigation if the product or service was brought to market.

Some regulators are proving willing to take enforcement action in this area. For example in 2022, the US Federal Trade Commission ordered the company formerly known as Weight Watchers to delete algorithms derived from personal data unlawfully collected from children. In order to mitigate the risk of any enforcement action, organisations can consider creating 'data protection gateways', making a data protection review a pre-requisite for obtaining project approval and funding.

Ensure cross-stakeholder collaboration: Data protection compliance is not just for lawyers, privacy or compliance professionals — it also involves research, development and product teams. When data protection is siloed from R&D and product departments, this can lead to protecting the product as designed, instead of designing the product to comply with data protection requirements. Establishing processes and procedures that see those conceptualising, de-

(Continued on page 8)

(Continued from page 7)

veloping and launching products or services working alongside data protection experts can help identify, address, and mitigate issues both early on and as they arise throughout its lifetime.

What works and what is required will vary between organisations. One option is formally embedding an individual with data protection expertise in research, development and product teams to facilitate continuous, or at least frequent, dialogue on how data protection requirements should manifest in the product or service.

Revisit, review, revise: Data protection by design and default is a dynamic process. Products and services evolve over time either by design or necessity as regulatory and commercial landscapes shift.

To ensure lifecycle-centric data protection compliance, organisations might consider establishing programmes to revisit, review and revise data protection compliance in the context of a specific product or service that goes beyond traditional auditing for compliance with existing policies and processes. Many organisations can do this through periodic and event-based 'trip wires'. For instance, they can perform set reviews of existing products and services, and use specific events or junctures to trigger additional analysis, existing determinations being revisited, and necessary revisions being made. Common triggers might include when there are planned changes to the way in which the product or service operates, the personal data processed, or the purposes for which data are used. Once established, organisations should consider revisiting their 'tripwires' at minimum intervals. This will allow triggers to evolve in response to emerging enforcement priorities, regulatory guidance, and market best practice. It will also allow organisations to ensure that they consider the viability and desirability of applying new privacy-enhancing technologies to existing products and services as they emerge.

> ***"To ensure lifecycle-centric data protection compliance, organisations might consider establishing programmes to revisit, review and revise data protection compliance in the context of a specific product or service that goes beyond traditional auditing for compliance with existing policies and processes."***

Identify, articulate and address design priorities and guardrails: Organisations should establish and communicate what they are aiming for. Effective design is integral to discharging many EU and UK GDPR obligations and essential to meeting consent, transparency, and individuals' rights request-related requirements. 'Dark patterns' or 'nudges', in particular, are increasingly scrutinised and may present a real risk of regulatory attention given the potential to fall foul of the EU and UK GDPR's overarching fairness principle. Perhaps best developed in the context of cookies consent frameworks, design guidelines from the French CNIL for ensuring consent is obtained in an even-handed manner can be leveraged more broadly.

Similarly, the EU and UK GDPR require that privacy notices are intelligible and easily accessible. Good design and design testing can go a long way to meeting those requirements. To weave best practices together in an actionable format, organisations might consider creating non-exhaustive, indicative design guardrails that can evolve over time, with concrete examples of best practice and what to avoid, drawing on relevant guidance.

Design for safety: One of the core elements of data protection by design and default is robust technical and organisational measures to safeguard personal data. It is important to design for safety, rather than implementing security as an overlay. Organisations may want to ensure that security is understood broadly. Designers and developers are often accustomed to considering user goals and privacy risks arising from unauthorised access, but not necessarily how to counter harmful goals of known users or how to provide actionable information to victim users.

In addition to ensuring that security is embedded throughout the development and design process, organisations might also want to ensure that those assessments address such considerations as power imbalances between users; whether users can easily identify other individuals and their actions; and safeguards against third party surveillance. Organisations should also be mindful of sector specific obligations outside the data protection sphere. For example, the forthcoming EU Cyber Resilience Act is set to require certain device manufacturers to ensure minimum security standards (e.g., eliminating default usernames and passwords) are met and that cybersecurity concerns are considered throughout the product lifecycle: planning, design, development, productions, delivery and maintenance. In the UK, the Product Security and Telecommunications Infrastructure Act imposes similar requirements, and covered businesses should monitor for forthcoming secondary legislation that will set out more detailed requirements.

Document considerations and decisions: Organisations should ensure that they receive credit for their data protection by design and default work. The accountability principle requires organisations to be able to demonstrate compliance with the EU and UK GDPR's requirements. Under the proposed EU Cyber Resilience Act, documenting cybersecurity risks is anticipated to be mandatory for certain device manufacturers. Documenting data protection considerations and decisions in a clear and accessible

(Continued from page 8)

way will be key to meeting these requirements, but also positioning an organisation to be able to address Supervisory Authority or individual queries if and when they arise.

While there is no one size fits all approach, organisations might consider establishing assessment and decision templates. These may not only help ensure that EU and UK GDPR and internal standards are applied consistently across different business areas and service lines, but may also help organistions to track and manage changes more easily over time. Good governance, like in other areas of compliance, might also require periodic audits or sampling to ensure any internal documentation requirements are being adhered to.

Provide ongoing learning opportunities — prioritise training: Creating cross-stakeholder understanding and alignment can be beneficial. Shared training across functions can help ensure that there is a common baseline knowledge of the relevant regulatory landscape on which to build data protection by design and default.

Organisations might also want to ensure that training is bi-directional. Traditionally, data protection training has been given to non-data protection specialists, but product development and other technical training for those advising on, and responsible for, data protection implementation has been less common. This type of training can allow those driving data protection compliance to better understand both the broader process in which they participate, as well as specific technical dimensions that might aid their ability to advise on, and implement, data protection by design and default effectively.

Understand the international landscape — Look beyond the EU and UK GDPR: Whilst the EU and UK GDPR have one of the most explicitly articulated data protection by design and default requirements, the need for robust privacy by design is increasingly global. Although the United States still does not have a general federal privacy law but rather a patchwork of state and sector-specific laws, the US Federal Trade Commission (along with several state regulators) has stated that it is focused on stopping deceptive and unfair practices, including dark patterns, noting the risk that user interfaces can subvert consumer autonomy and decision-making.

While presenting an increased regulatory risk for organisations, the global proliferation of laws that complement the EU and UK GDPR's data protection by design and default requirements may make it easier to secure intra-organisational buy-in for investment and implementation. In short, what is expected by the EU and UK GDPR may increasingly be expected elsewhere; opportunities for regulatory arbitrage may decrease over time; and complying with the EU and UK GDPR as a benchmark standard might in some cases be a cost efficient way to future proof, or at least mitigate risks associated with, a product or service. To keep track of this fast-moving area, organisations may want to ensure that their regulatory tracking covers changes that could feed into data protection by design and default-related expectations in the future.

Robert Maddox and Stephanie Thomas
Debevoise & Plimpton LLP
rmaddox@debevoise.com
sdthomas@debevoise.com