Privacy by Design... by design

Simply Privacy

As agencies increasingly adopt more agile and 'by design' approaches to product and service design, privacy functions must adapt their approaches to engaging with project teams to effectively influence data practices and outcomes. This guidance is intended to help privacy professionals and their teams put Privacy by Design into practice, outlining the factors that we think can influence a successful privacy function.

Privacy by Design methodology

Privacy by Design (**PbD**) allows for a more responsive and proactive approach to privacy management, adapting privacy settings to address positive or negative changes to privacy risk as project design and outcomes evolve. It also ensures a more meaningful risk management process, by requiring engagement with an agency's privacy function throughout the project lifecycle, not merely at a single (often belated) point in the process.

1. **Proactive not reactive, preventative not remedial**
Privacy needs to be considered early in the project lifecycle. Privacy considerations should help drive the design rather than being tacked on at the end to remediate apparent privacy risks.

2. **Privacy as the default**
The default setting of any design should protect individual privacy. This means privacy-protective settings (such as data minimisation and use limitation) should be the starting point.

3. **Privacy embedded into design**
Privacy should be a foundational element in the design of a product or process and should be so integral to that product or process that it will not function if privacy settings are altered or removed.

4. **Full functionality – positive sum, not zero-sum**
Privacy requirements should not be delivered at the expense of other core functionality. This is not a trade-off. Instead, privacy requirements should support and enable the delivery of other requirements.

5. **End-to-end security – lifecycle protection**
Data protection should be ensured at every stage of the information lifecycle for a new product or process, including collection, storage, use, disclosure, and disposal.

6. **Visibility and transparency**
There should be visibility of the privacy risk assessments, design decisions and privacy controls established for a product or process. This will increase trust in the project.

7. **Respect for user privacy – keep it user-centric**
Where a product or process will be used by individuals – such as customers – those individuals and their experience should be central to design decisions.

Implementing Privacy by Design in practice

Implementing Privacy by Design in practice, and successfully integrating privacy into agile work environments and processes, requires a considered approach. Several factors will impact on the success of a Privacy by Design approach and, more generally, the success of an agency's privacy function.

Definition of accountabilities
The agency must clearly define roles and responsibilities, accountability and ownership, and escalation processes. The privacy function and the project team should be clear as to who is accountable for privacy risks, who is responsible for privacy mitigations, who needs to be consulted about privacy compliance, and who should be informed of privacy outcomes. If this is not defined, there is a tendency for project teams to push all responsibility and accountability to privacy functions. This is neither appropriate nor sustainable.

Strategic intervention
The privacy function must be involved at the right times in the project lifecycle. Most importantly, the privacy function needs to engage early in the design stages of a project, to ensure that privacy requirements can be properly considered, and embedded into a product or process from the outset. The privacy function should attend project design meetings and be willing to engage early in design conversations. Privacy advice at early stages can be principles-based and theoretical. The privacy function should also be engaged at critical later stages of the project, including testing and launch. At these later stages, privacy advice should be more detailed and practical.

Responsiveness and timeliness
The privacy function must be capable and willing to be responsive and available to the project. A failure to be responsive – such as delays in returning privacy advice in time for important project decisions to be taken – could result in the project team bypassing privacy requirements, avoiding privacy risk assessments, or reducing overall engagement with the privacy function. Capability relies on sufficient resourcing and allocation of priorities. A privacy function will be less responsive if it is under-resourced or distracted by the wrong priorities.

Adaptability
Change is a defining feature of most projects. Over time, project requirements will change, outputs will be updated according to changing project objectives or new design limitations, timeframes will be shortened or lengthened, or external factors will alter the project risks. The privacy function must be attuned to these variables and able to adapt. This may include adapting the way the privacy function engages with the project or being willing to review and update the privacy risk assessments, recommendations and advice being delivered to the project.

Enablement and support
The privacy function should enable the project team to get privacy right, by complementing privacy risk assessments and advice with clear guidance on how to put privacy principles into practice. This guidance should be focused and practical, not theoretical. Privacy training for key project teams or team members could further enable positive privacy outcomes, and provide important relationship building opportunities for the privacy function.

Content
Privacy risk assessments must consider the breadth of privacy issues raised by a project. Privacy means more than privacy law and should include related issues such as ethical considerations, indigenous privacy sensitivities, and the importance of data ownership and governance. This may mean collaborating with other subject matter experts, such as information security and data governance experts. This also includes ensuring that the privacy function sees the wood and the trees - appropriately considering the big picture privacy risks as well as the detailed process risks.

Risk-based targeting
Privacy efforts and interventions should be targeted based on clear and consistent thresholds, such as the likelihood of harm to individuals concerned. The privacy function should "pick its battles" and recognise that not all privacy risks are equal. Further, the approach should reflect that privacy is one of many risks the agency must address. The Privacy Act itself facilitates this approach, providing that the right to privacy may be balanced against the general desirability of a free flow of information and the right of business and government to achieve their objectives in an efficient way.

Pragmatism
The privacy function must put itself in the project's shoes and ensure that core project outcomes and objectives are well-understood. This will allow for the delivery of pragmatic privacy advice that enables the project team to meet its objectives in a privacy-protective way. Recommendations should be clear and practical, not theoretical. Rather than advising a project to minimise the data it collects, tell the team what data elements to remove.

Balance
Privacy can create both risks and opportunities for a project. In many cases, good privacy practices will assist rather than hinder the achievement of a project's goals. Further, in some cases, changes to a product or process prompted by other factors could have a positive impact on privacy compliance. It is just as important for a privacy risk assessment to identify and highlight privacy opportunities and improvements as it is to call out the compliance risks.

Appropriate communication
Privacy advice and risk assessment should be articulated and communicated in a way that is meaningful for, and understandable to, the target audience. Documents should be as short as possible, with risks and recommendations clearly outlined early. Privacy messaging to operational staff should be pragmatic, practical, and detailed, whereas privacy messaging to senior leaders should be strategic and high-level.

Visibility
Internal privacy risk assessments and controls are important to ensure privacy is protected, but if they are not visible to the people concerned, they do nothing to build trust and confidence in a product or process. Visibility means making privacy risk assessments public or, if this is not possible, making efforts to provide the public with assurances that privacy has been designed into the product or process and how this has been achieved.

Simply Privacy is a specialist consultancy providing privacy advice, strategy and consultancy services to public and private sector organisations. We believe in a holistic approach to privacy practice and we work with our clients to ensure that privacy solutions fit with their business needs and wider goals.

Please note that the contents of this checklist are not legal advice, and should not be taken as such.

Simply Privacy