Applying the Positive-Sum Principle for Successful Privacy by Design Outcomes

Dan Goldstein, CIPP/E, CIPP/US
Kamal Govindaswamy, CIPP/US
Katharina Winkler

iapp

Privacy and data protection professionals have spent a great deal of time and effort in the last few years preparing to comply with new international regulations such as the European Union's General Data Protection Regulation, the Network and Information Systems Directive and the upcoming ePrivacy Regulation. With GDPR and NIS recently in effect, and the ePrivacy Regulation fast approaching, there has been an ongoing buzz of activity, with organizations pressing to build and adjust their privacy and data protection programs in advance of the new rules. It's not unfamiliar territory to many; we've seen similar frenzies in the past ahead of new rules such as PCI DSS and the HIPAA privacy and security rules in the U.S.

As technologies such as the cloud, smart devices and the internet of things gain continually increasing rates of adoption and pervasiveness, traditional privacy and security approaches are in serious need of reevaluation. In this environment, effective and sustainable management of privacy and data risk should be a key objective.

Building a positive-sum mindset for privacy-aware design and development

One of the most important factors for building an effective and sustainable privacy program is encouraging — even requiring — proactive collaboration between cross-functional stakeholders. Such collaboration should encourage innovative approaches to privacy risk management that support business initiatives without compromising security objectives or compliance obligations. And while developers and process designers can view privacy and data security as barriers to innovation, both privacy and security principles must be embraced in order to implement new solutions.

An engaged and impactful privacy program will feature team members that not only embrace innovation, but also possess the requisite level of inquisitiveness, experience and thought leadership to apply innovative thinking about privacy to enhance new processes and technology. These individuals will benefit new initiatives by:

- Applying new strategic approaches to meeting business or technology objectives without compromising privacy risk management or compliance objectives.
- Providing the requisite leadership to drive the development of tactical implementation of those new strategic approaches.
- Driving adoption of innovation throughout the privacy team in order to eliminate complacency with traditional compliance approaches and encouraging contributions throughout the team.

Taking this into consideration, the concept of a "positive-sum" approach in which stakeholders share a single set of objectives

driving the design, development and implementation of business initiatives or technologies, provides a strategic boost toward attaining effectiveness and sustainability. And while optics are important, the real-world payoffs in terms of knowledge-sharing, teaming across functions and building strong foundations for further collaboration, are hard to deny.

Implementing a positive-sum approach and achieving downstream results is not without challenges, however, as it requires that privacy and data protection are viewed as business and technical requirements in the beginning stages of planning and designing new initiatives and systems that support business objectives. A key component that will drive your efforts toward achieving a positive-sum privacy program is the proactive engagement and collaboration between the business teams, the information technology development team, the data privacy team and information security.

Proactive engagement

Privacy's engagement of the business and development teams must be based on a foundation of trust and shared measures for success. It is important for the business and technology teams to understand that the privacy team is not there to create hurdles to their objectives, but to help them successfully navigate the complexities of the GDPR and its privacy by design provisions, while improving data processing activities in ways that benefit both the business and the individuals.

In order to gain that essential seat at the table in the early planning stages of new processes or technology solutions, privacy teams must be committed to proactive engagement with business and technology leaders. While privacy by design might be built into procedures or up-to-date system development lifecycles, privacy will need to engage development teams to earn their requisite influence. Proactive engagement results in the privacy team:

- Gaining an understanding of business and technology initiatives at a stage where privacy and data protection will be viewed as functional requirements for the successful build and execution of the initiative.
- Establishing status as a key participant in and contributor to the initiative.
- Establishing business and technology stakeholder confidence in privacy as a partner and enabler as opposed to a hurdle posed by bolted-on legal or compliance demands.
- Embedding privacy into the design of new business processes and technology solutions.

Collaboration with information security

An organization's ability to implement sustainable security safeguards that truly protect personal data has always been a key objective of privacy programs. Current trends in use of cloud, mobile computing, big data and IoT make that objective not only more significant, but also much more challenging to achieve. In order to contribute to and collaborate successfully with information security, the privacy team should incorporate information security knowledge within the privacy team. A team member with information security background is a tremendous asset to the privacy function. This team member enables deeper discussion of technical information security issues and solutions and helps position privacy as a valued contributor to security solutions, rather than as an outsider seeking to drive greater security.

An additional opportunity to engage in cross-functional collaboration is through data mapping. The privacy team should undertake data mapping exercises that focus on the flow of personal data throughout the lifecycle of existing or planned processes and systems. Well-executed data mapping exercises will produce visual depictions of data flows, identifying flows within the organization and out to its third-party and cloud-based ecosystems. These maps will allow information security greater visibility so that appropriate safeguards can be designed and built into the process or system.

Operationalizing the positive-sum approach

Assessing and mitigating risk of harm to individuals

In order to fully implement privacy by design and positive-sum objectives, business owners — in collaboration with the privacy team — must use risk management tools such as privacy threshold assessments and (where applicable) data protection impact assessments at the outset of a project to assess, identify and reduce privacy risks to individuals. Privacy threshold assessments facilitate the determination of risk of harm posed to the individuals by the processing activity being designed. If the processing poses a high risk of harm, the full DPIA should be conducted to identify means to reduce those risks.

The privacy threshold assessment should score or rank the risk associated with the processing based on the characteristics of the processing activity. Considerations may include:

- The type of personal data being processed.
- The estimated number of individuals whose personal data will be processed.
- Whether personal data will be shared or disclosed to organizations or parties who did not previously have routine access to the personal data.
- Whether the project will involve using a new technology that may be perceived as intrusive by individuals.
- Whether the project will involve automated decision-making.
- Whether the project will involve profiling of individuals.
- Whether the project will require the combining of datasets from disparate data processing operations performed for different purposes.
- Whether the project will require contacting individuals in ways that may be considered intrusive.

If the scoring reaches the threshold level established by the privacy team (or legal or compliance teams), a full DPIA should be conducted. As necessary, based on the outcomes of the DPIA, adjustments to the processing activity should be made or appropriate privacy enhancing controls introduced.

Proactively mitigating the risk of harm through privacy controls

Certain privacy controls must be introduced in the design phase regardless of the risks posed to the individuals by the processing activity. These include core privacy concepts, such as limitations on types of data and processing, proper transfer protocols and enforceable data retention periods. In order to establish these privacy controls, the business owners,

privacy team and process design teams must answer the following questions:

- **What type of personal data is being processed?** Prior to implementing a new process or technology that processes personal data, or making changes to existing processes or technologies, the teams must identify and document the types of personal data being processed. This will enable the determination of what types of organizational or technical safeguards are appropriate to secure the data, considering the risks to the individuals and the company.

- **What is the purpose of the data processing?** The teams will need to identify and document the purpose of the processing and facilitate the design and implementation of controls to limit personal data collected to that which is necessary to fulfill the intended purpose. For example, if the personal data necessary to fulfill the purpose can be limited to an individual's name, date of birth and gender, the individual should not be asked to provide information about annual income.

- **What information is required for the notice?** Business owners should collaborate with the privacy team (or the organization's compliance or legal department) to verify that any required privacy notice contains adequate information to meet applicable notice requirements, such as GDPR Articles 13 and 14. Teams should consider any foreseeable secondary purposes for processing the personal data in the design phase so that these purposes can be included in the applicable privacy notice; and, of course, the information provided in the privacy notice should be clear, readily accessible and easy to understand.

- **How will the personal data be collected?** Business owners must work with the privacy team to identify how personal data will be collected in order to determine the point and manner by which privacy notice should be provided and what security measures should be applied in the collection process.

- **What is the legal basis for processing?** Business owners and the privacy team (possibly in collaboration with the organization's compliance or legal department) must identify and document the legal basis for processing the personal data (e.g., legitimate interest, consent, contractual necessity). This will help determine how notice will be provided (e.g., in a standalone notice, in a consent document, or in a contract).

- **What data transfers will take place?** Transfers of personal data require collaboration between the business owners, privacy, IT development teams and IT security. First, business owners must identify and inform the privacy team of third parties with which the personal data will be shared, including any cross-border transfers of personal data. This enables the implementation of appropriate transfer mechanisms and contractual provisions as necessary. It also provides information about data sharing and transfers that must be communicated to individuals in the privacy notice. Critically, the business owners and privacy team must collaborate with the development team and IT security with regard to transfers to ensure that proper safeguards are in place to protect the data while in transit to third parties.

- **How long should the personal data be retained?** Data retention — and destruction at the end of the retention period — can be notoriously difficult to define and even more difficult to put into effect. During the design phase, business owners must work to identify demonstrable criteria to support the retention of personal data for a specified period. They must then work with the design team to determine whether there are automated means to delete the personal data at the end of that period or define a manual process to do so.

By identifying all the described aspects of the processing activity before new technologies, systems or processes are introduced, businesses not only meet applicable GDPR requirements, but realize a number of ancillary benefits. These benefits include establishing a general awareness of data privacy in the minds of key stakeholders and driving fundamental privacy and personal data processing behaviors out into the business culture. The ultimate effect is that this filters down to the individuals and generates an increased level of trust in customers, prospects, employees and others.

Proactively mitigating the risk of harm with tailored security safeguards

The privacy threshold assessment and, if conducted, the full DPIA will indicate the level of security controls appropriate to the processing of personal data taking place. At this stage, engagement and collaboration with the information security team is critical. Successful integration of security controls that are appropriate to mitigate the risks associated with the personal data processing activities are essential. Less than adequate security controls will result in unnecessary increased harm to the individuals and significantly increased regulatory, financial and reputational risk to the business.

A key tenet of the positive-sum approach is that an organization shouldn't have to make unnecessary compromises between security, privacy and business functionality. Diligent research, planning and execution should help accomplish goals across all three areas in equal measure.

Privacy enhancing technologies and appropriately designed security solutions or processes are key to safeguarding privacy without compromising delivery of business or security objectives. At a minimum, the following core security components should be considered:

- **Identity and access management**

  Access to personal data being processed must be limited to those employees, vendors or other third parties for whom access is required in order to perform specified actions. IAM helps ensure verification of users (identification, authentication) and that access is provided only as necessary (least privilege or need-to-know) for the right duration and to the right people or resources. Importantly at this stage, the security and design teams must keep in mind that AIM tools, by their very nature, require the processing of personal data attributes associated with the individuals for whom access is being granted. As such, the privacy rights of these individuals must also be considered and appropriately addressed.

  A good privacy program will inform (e.g., via an employee privacy notice) those who must have access to the new systems, applications, or processes

being designed, that their access is dependent on the processing of their own personal data for purposes of access management.

There have also been significant advances to help address this privacy/security dichotomy. In particular, standards continue to be developed to support privacy and business needs. There are IAM solutions currently available that implement these standards and as the standards evolve and mature so too do the solutions. Security and privacy programs should consider these standards and solutions as key enablers of the privacy and business requirements.

- **Encryption, pseudonymization and anonymization tools**

  The security, development, business and privacy teams must collaborate to determine the necessity and feasibility of implementing privacy enhancing technologies.

  Reversible encryption, for example, can be used to pseudonymize personal data when at rest (in storage), in transmission, or in use (in computer memory for example). Encryption keys are stored securely and become accessible when the original data needs to be available in specific authorized contexts to authorized users. Irreversible encryption such as password hashing can be used when the original data should not be available under any circumstances.

  Data masking is another excellent pseudonymization tool in which certain parts of data are masked in specific situations and to specified users (e.g., replacing all but last four digits of a U.S. Social Security number with asterisks). Full data can be shown in limited cases after step-up authentication.

  Tokenization is a privacy-enhancing technology that can be applied during the design stage to replace personal data with values (tokens) that cannot be used to identify an individual, but can still be applied to achieve the objectives of a processing activity. For example, a secured lookup table can contain a mapping between the original data and tokens to enable the retrieval of the original data for processing. Tokenization is an important solution used by retailers to comply with the Payment Card Industry Data Security Standard.

  As appropriate, these controls should be applied not only to data at rest within the businesses systems and databases, but also to transfers of data to third parties or to a business's own off-site databases or cloud service providers.

  It's important that the development and data security teams are aware in the design phase that solutions such as encryption do not need to be applied to entire systems or even specific records, but for purposes of privacy protection can be applied only to specific fields that identify an individual.

- **Testing throughout development**

  The effectiveness of the key administrative, technical and physical safeguards protecting personal data should be tested at regular intervals throughout the development of a new processing activity. This should include undertaking threat and vulnerability testing, such as security penetration,

web vulnerability and resilience testing as appropriate given project progress. Project teams should collaborate to identify and implement appropriate modifications to application, system or process security controls, taking into consideration the results of tests performed and new and evolving threats.

All of the above privacy-enhancing technologies are viable options to help deliver privacy objectives without inhibiting business needs or compromising security objectives. It is important, however, that appropriate due diligence is conducted before selecting the right option(s) given the specific business and its operational characteristics. Given the broad definition of personal data under GDPR and the complexity of the data processing environment, an organization may need to consider implementing a variety of solutions. Choosing a sub-optimal option may result in unnecessary inhibition of business needs and defeat the positive-sum principle.

Applying industry expertise for positive-sum outcomes

Successfully reaching positive-sum objectives requires that industry-specific knowledge either resides in or is shared with the privacy, security and IT development teams.

Pharmaceutical and biotechnology provide great examples of industries in which privacy professionals must pay particular attention to rules and regulations that are outside of the traditional privacy focus when planning certain processes and technology solutions. For example, the EU Clinical Trials Regulation puts affirmative obligations on sponsors of clinical research that may not always easily align with more obvious data privacy obligations. Sunshine acts (financial transparency rules and regulations) provide similar challenges. In some instances, this may require that the privacy team consider whether GDPR Article 6(1)(b) might provide a legal basis for processing the personal data and how that impacts privacy by design considerations such as collection limitation, notification and/or obtaining consent. Industry expertise and an understanding of how to navigate these complexities is essential to achieving positive-sum outcomes.

The health care industry provides similar complexities calling out for industry knowledge. For example, deep experience with clinical workflows in a health care provider setting is essential for the collaborative business, privacy, IT development and security teams to develop and operationalize good privacy and data security controls. Substantial working knowledge of electronic health records environments and digital health initiatives will have a similar positive impact on the success or failure of new personal data processing initiatives.

Travel and leisure is another area with some unique requirements. For example, requests for wheelchair assistance at an airport or special meals on a flight may not require specific, informed, demonstrable consent even though these requests by their nature indicate sensitive personal data. However, it is of course crucial to the individuals and to the airline that such information is appropriately secured. It is highly important to efficient operations and risk mitigation efforts that these unique outlier requirements are understood when designing new processes that may include personal data.

Conclusion

A privacy program that produces positive-sum results in the design, development and deployment of new processing activities is a desired outcome for all privacy professionals — particularly those tasked with leading a privacy program and working across multi-disciplinary functions to achieve results. While positive-sum outcomes are reasonably easy to envision, they take hard work and cross-functional cooperation to achieve. The inclusion of privacy by design in GDPR has added a new and necessary impetus to realize the positive-sum principle. This requires planning in terms of organization and staff and socialization across diverse business, IT and security functions. With proper planning and execution, a positive-sum strategic approach puts compliance objectives within reach and leads directly to the ancillary benefits of a higher level of individual trust and enhanced business reputation.

Dan Goldstein, CIPP-US, CIPP-E,
Co-Founder and Partner, Tueoris

Dan is a co-founder and partner of Tueoris. He advises clients operating in complex business and regulatory environments on privacy and data risk mitigation strategies and solutions. He focuses on enterprise-wide information risk management strategies and solutions in accord with applicable requirements across industry. His career has centered on guiding U.S. and multinational clients through complex international data protection requirements in order to provide business solutions that can be implemented across large organizations. He is a member of the State Bar of California, and has over 15 years of professional experience focused specifically on data protection.

Dan is a graduate of the University of California, Los Angeles and the Golden Gate University School of Law. He is a member of the State Bar of California. He is a Certified Information Systems Security Professional (CISSP) and a Certified Information Privacy Professional (US and European certifications).

Kamal Govindaswamy, CIPP-US,
Co-Founder and Partner, Tueoris

Kamal is a co-founder and partner of Tueoris. With over 20 years of consulting services experience, Kamal's information security and privacy consulting philosophy is rooted in his facts-based-pragmatism for furthering his clients' business agility and objectives. He oversees our consistent track record and exceptional focus on delivering outcomes that truly matter to our clients, for each of their business, risk or regulatory compliance contexts. His specialties include security or privacy programs — development and implementation of strategies, security or privacy risk or compliance assessments, identity management — strategy or roadmap development and program management, security or privacy operations — develop strategy for and implement monitoring and response capabilities and regulatory compliance. His clients include large and medium size organizations across health care or life sciences, retail, financial services and consumer business industries.

Katharina Winkler
Consultant , Tueoris

Katharina is educated in U.S. and EU privacy and technology law. She is a German trained lawyer (Volljuristin) and obtained a LL.M. degree in Intellectual Property and Information Technology Law from the Fordham University Law School in New York City. At Tueoris, she helps multinational clients across industry (including pharmaceuticals and biotech) to navigate complex EU and global privacy requirements.

Katharina previously worked in the digital business department at an international law firm where she drafted e-commerce policies and software contracts and advised German and U.S. tech businesses on EU consumer and data protection laws. She also worked at the Fordham Intellectual Property Institute and spent three months at a law firm in New York City where she drafted memoranda on the EU-US Privacy Shield and other international regulatory developments.