WHITEPAPER

A Guide for Structuring and Implementing PIAs

Six steps for your next Privacy Impact Assessment

TRUSTe Inc.

US: 1-888-878-7830

www.truste.com

EU: +44 (0) 203 078 6495

www.truste.eu

CONTENTS

SUMMARY

Privacy is going to get more complex before it gets simpler.

Data continues to flow from more individuals through more channels. New and innovative practices of exchanging data at ever-increasing speeds result in the collection of personal information that may expose companies to risk. Information from customers and employees that businesses took for granted just a few years ago is now at the heart of consumer complaints, data breaches and Federal Trade Commission (FTC) penalties.

The privacy office or privacy team is responsible for ensuring that the organization uses personal data ethically and in a manner consistent with its privacy policy. The Privacy Impact Assessment (PIA) is a process of for identifying, assessing and mitigating privacy risks for a specific product, service or system.

This paper introduces businesses of all sizes to the PIA – the standards they should follow, the kinds of data they should include, the questions they should answer and the areas they should analyze. Privacy officers, executives and project managers will take away insights for assessing the impact of privacy in their own organizations and ensuring that they are being careful enough with personal data.

THE EVOLVING PRIVACY LANDSCAPE

The rise of the Internet has greatly affected the role businesses play as stewards of the data that customers have entrusted to them. The coming Internet of Things will affect this role even more.

Every day, for example, users around the globe generate nearly 2.5 quintillion bytes of data. In fact, 90 percent of the data in the world today has been created in the last two years alone. About 75 percent of that data is unstructured – that is, random and difficult to index – such as social media, news and consumer preferences.

Big data, as we call it, has not come about suddenly, but gradually over time. It presents new opportunities not only in science but also in business, as more companies try to mine and make sense of it for commercial advantage. With data being exchanged globally in such large volumes, in new and creative ways and at a lightning-fast pace, preventing the misuse of customer and employee personal data becomes more complex. APEC Cross Border Privacy Rules (CBPR), the proposed General Data Protection Regulation in the EU and other frameworks are establishing guidelines for the proper use of personal data. Keeping up with regulatory change is yet another layer of complexity that the privacy office must address.

More data means more privacy concerns

The conversation about data leads quickly to privacy concerns, as recent research by Harris Interactive[1] shows:

- 92% of US Internet users worry about their privacy online
- Only 55% of US Internet users trust businesses with their personal information online
- 89% of US Internet users avoid businesses that do not protect their privacy

The main lessons for businesses handling personal data are: 1) to be as transparent as possible to customers when providing notice about how they are using that data; and 2) to provide customers with choice(s) and control over how their personal data is used.

That may seem obvious, but several high-profile breaches of trust have made the headlines.

- Facebook assured users of the social network that access to their profile information could be restricted to "Friends" or "Friends of Friends;" however, Facebook further shared that profile information with third-party apps. In addition, Facebook designated as publicly available certain user profile information that previously had been subject to privacy settings. As a result of these unfair and deceptive practices, the 2012 FTC consent decree required Facebook to obtain bi-annual privacy audits for 20 years and to obtain users' consent before sharing beyond privacy settings.[2]
- Google received complaints of deceptive tactics and violations of its own privacy promises to customers when it launched its social network, Google Buzz. According to the settlement, Google must avoid future privacy misrepresentations and submit to regular privacy audits for the next 20 years.[3]
- The social networking app Path was found to collect personal information from mobile device contact lists without the knowledge and consent of users. The app also collected personal data from children without first obtaining parental consent. The final FTC settlement imposed an $800,000 civil penalty on Path and requires that the company obtain independent privacy assessments every other year for 20 years.[4]

1 Survey conducted online by Harris Interactive on behalf of TRUSTe, Inc. (December, 2013)
2 "FTC Approves Final Settlement With Facebook," FTC, August 2012, http://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook
3 "FTC Gives Final Approval to Settlement with Google over Buzz Rollout," FTC, October 2011, http://www.ftc.gov/news-events/press-releases/2011/10/ftc-gives-final-approval-settlement-google-over-buzz-rollout
4 "Path Social Networking App Settles FTC Charges..." FTC, February 2013, http://www.ftc.gov/news-events/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived

With which types of data should we be most careful?

The misuse of personal data is what prompted the FTC investigation and actions mentioned above. Examples of personal information include contact information, social security numbers, driver's licenses, financial account information, individually identifiable health information, log-in credentials, device IDs, browsing habits and personal preferences.

The channels from which to collect this data are quickly becoming more numerous, and so are the opportunities to use it in tailoring offers, products and services. Highly visible sources include online webinars, website forms, online surveys and email campaigns; less obvious sources include mobile device geolocation and tracking, social media likes and shares, cookies, fingerprinting, email list purchases and mobile app preferences.

Within the organization itself lies a different set of concerns: the employee data that resides in such forms as job applications, payroll records and health care files.

Fair information practices (FIPs) are the foundation of most global data protection standards, which generally cover these concepts [5]:

- Consent
- Accountability
- Identifying purposes
- Collection limitation
- Use, retention and disclosure limitation
- Accuracy
- Security
- Openness
- Access
- Compliance

Many businesses routinely collect personal data without even thinking about it. Nevertheless, they have a duty to be aware that they are collecting it and that they have obligations to appropriately protect it.

5 "Creation of a Global Privacy Standard," Cavoukian, Ann, Ph.D., Information & Privacy Commissioner, Canada, November 2006, www.ipc.on.ca/images/Resources/gps.pdf

THE PRIVACY IMPACT ASSESSMENT (PIA)

The vehicle for evaluating an organization's awareness of how it handles consumer and employee information is the Privacy Impact Assessment (PIA).

The PIA is a decision-making process used by the privacy team to identify and mitigate privacy risks at the beginning and throughout the development lifecycle of a program or system. It helps a company to understand what personal data the company collects, why it has been collected and how it will be used, shared, accessed, stored, and retained. Depending on the scope of the project, it is helpful to create a personal data inventory to understand what data is collected and where it is stored; map how data flows through business processes and/or relevant systems; and update key policy documents (e.g., internal privacy policies and guidelines and external privacy notices).

In the UK, the Information Commissioner's Office (ICO) has published a document called "Conducting privacy impact assessments: code of practice [6]," which describes the benefits of conducting PIAs:

> "Privacy impact assessments (PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective PIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. PIAs are an integral part of taking a privacy-by-design approach."

The ICO's code of practice is exceptionally useful for practitioners, consultants and project managers tasked with conducting PIAs. It sets out in detail the perspective of regulators who assess privacy activities in organizations. The code guidelines for a PIA are applicable irrespective of country of origin. The code of practices is a valuable resource for creating and defining internal privacy-protective processes, and it also demonstrates that a privacy risk management process is in place should regulators conduct a data protection audit.

There are six steps involved in the PIA model:

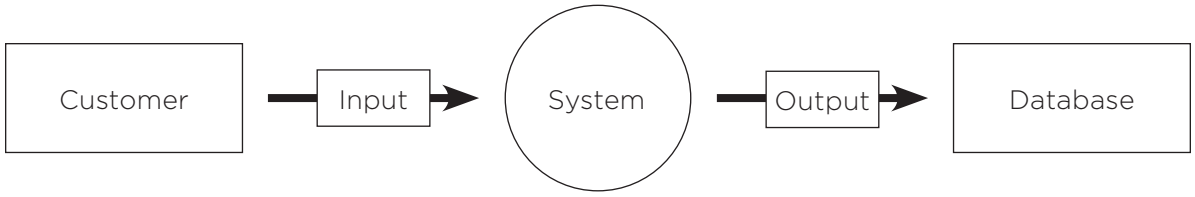
1. Identify the need for a PIA with a Privacy Threshold Analysis (PTA)

Although this may seem self-evident, it is a useful step. If there is no substantial privacy impact to a given activity, there may be no need to conduct a deeper dive into the program or system. Therefore, when reviewing assets within a particular business unit (e.g., business process, application or website), it is helpful to conduct an initial Privacy Threshold Analysis (PTA) for each asset. The answers to the PTA questions will determine which assets collect or use personal data in a way that requires further analysis in a PIA and they also determine which are out of scope for further review.

PTA questions are high-level and cover the type of data that is collected and used, how it is transferred, where it resides, which geographic regions will have access to it, how it will be used, obligations to individuals, involvement of third-parties and changes to the company's written policies and contracts.

If the answers to PTA questions demonstrate that personal data is collected and used in a manner that requires further analysis, then the privacy team will complete a PIA questionnaire with the input from the business. This questionnaire includes more specific questions about how the personal data is collected, used, transferred, stored, retained, shared and disposed of. Once the PIA questionnaire is completed, the privacy team will continue to amend it as the business informs them of major changes to the product, service or system: e.g., additional personal data collected, merger of data sets, merger of systems, decommissioning of a system.

6 Version 1.0, published February 2014, p.3, http://ico.org.uk/about_us/consultations/-/media/documents/library/Corporate/Research_and_reports/draft-conducting-privacy-impact-assessments-code-of-practice.pdf



In its simplest form, data mapping is fairly straightforward concept. However as organizational structure becomes more complex and changes over time, understanding the flow of personal data can become quite difficult.

2. Describe the information flows (Data Mapping)

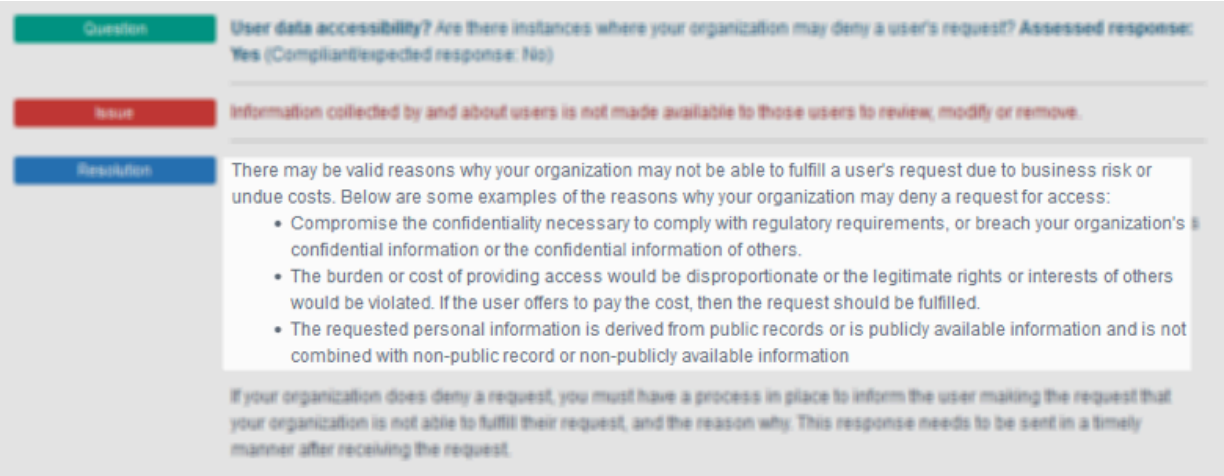
It is important to understand how personal data moves through a particular business process or system. Many organizations have already documented network maps and system diagrams. Similarly, to support a PIA, data mapping focuses on the ways in which data flows into, through and out of a particular business process or system.

The resulting data map precisely answers questions about the personal data collected, the business purpose(s) behind collecting it, sources of personal data, where data is stored, with which systems data is shared and who can access the data both internally and externally. Data mapping assists the privacy team with completion of PIAs.

3. Identify and assess privacy-related risks

Having identified the activity and the nature of the personal data involved, the next step is to identify risks, which may arise in a number of ways:

- Relative to the type of personal data being collected
- When requiring the collection of personal data instead of making it optional
- When storing personal data unnecessarily, especially if it is sensitive
- When providing access to personal data
- Where notice and choice to an individual is not adequate
- When security controls are insufficient
- When data quality is compromised
- Because of inadequate policies and standard operating procedures and improperly set consumer expectations
- When a data processor transitions to a data controller
- When personal data is in identifiable form rather than de-identified, anonymized or pseudonymized.



Establishing open channels of communication with all stakeholder groups ultimately leads to a more efficient PIA process.

This step includes specifying how the organization categorizes risks (i.e., low, medium, high). It also helps in explaining risks to other stakeholders in the organization, such as Product Management, Sales, Marketing and Engineering. Stakeholders can then understand how the risk affects a particular product, service or activity, and they can educate their teams and build in appropriate privacy protections.

4. Identify and evaluate solutions (remediation)

When gaps are found, the privacy team then assists the business owners in putting together a remediation plan. This includes a prioritization of outstanding privacy risks that need addressing, identification of which policy, procedure, process or feature changes should be implemented.

Some risks, of course, cannot be eliminated completely by the team, so they require escalation to executives who have the authority to accept risk based on the company's risk posture. It is important to follow a documented remediation plan in case the organization needs to demonstrate later how it has addressed known privacy risks. A documented plan also helps employees maintain accountability for addressing privacy risks under their control.

5. Sign-off and record PIA outcomes

The gap analysis and remediation plan from the previous step become the PIA plan of record.

Compliant businesses document all aspects of the assessment extensively, except for areas ordinarily free of the burden of documentation, such as information shared under a non-disclosure agreement (NDA) or communication subject to attorney-client privilege.

Ultimately, the main value of the plan of record lies in keeping it accessible and useful the next time the same product or activity is up for review or if a problem arises. Maintaining the plan of record within a system of record preserves that value.

6. Integrate the PIA outcomes back into the PIA plan of record

The final step of the PIA process is to fill the identified gaps. Additional documentation is helpful to clarify the steps required to remediate and the individuals within the company who will oversee each remediation effort.

This is also the opportunity to document lessons learned from the PIA process for use in the next one. A carefully maintained PIA plan of record details the ground that has already been covered and reduces the risk in future efforts to gather information.

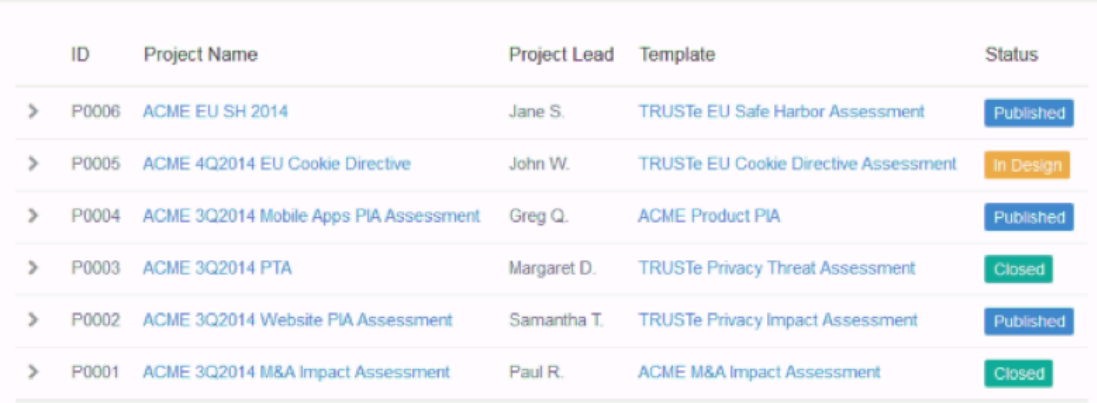
IMPLEMENTING PIA

The steps involved in setting up and implementing a PIA process vary greatly among large, medium and small businesses. The differences usually vary by the channels, products and services through which the company captures and uses data.

The PIA team

Assembling the right PIA team is essential, and the team should include some subset of these stakeholders:

- Executive sponsor of the budget behind the PIA effort – ideally the CPO, CEO, CISO, CIO or Privacy Counsel
- Privacy Office – to lead the effort from the legal perspective and track daily progress of the PIA
- Legal Team – Privacy Counsel or outside counsel with understanding of data governance and privacy
- Security Team (i.e., CISO or ISO) – to ensure proper technologies are in place
- Product Managers, IT managers, Marketing Managers
- HR – if the PIA includes employee data
- External privacy consultants – to offer outside perspective and compliance advice
- Employees responsible for managing systems that contain personal data



	ID	Project Name	Project Lead	Template	Status
>	P0006	ACME EU SH 2014	Jane S.	TRUSTe EU Safe Harbor Assessment	Published
>	P0005	ACME 4Q2014 EU Cookie Directive	John W.	TRUSTe EU Cookie Directive Assessment	In Design
>	P0004	ACME 3Q2014 Mobile Apps PIA Assessment	Greg Q.	ACME Product PIA	Published
>	P0003	ACME 3Q2014 PTA	Margaret D.	TRUSTe Privacy Threat Assessment	Closed
>	P0002	ACME 3Q2014 Website PIA Assessment	Samantha T.	TRUSTe Privacy Impact Assessment	Published
>	P0001	ACME 3Q2014 M&A Impact Assessment	Paul R.	ACME M&A Impact Assessment	Closed

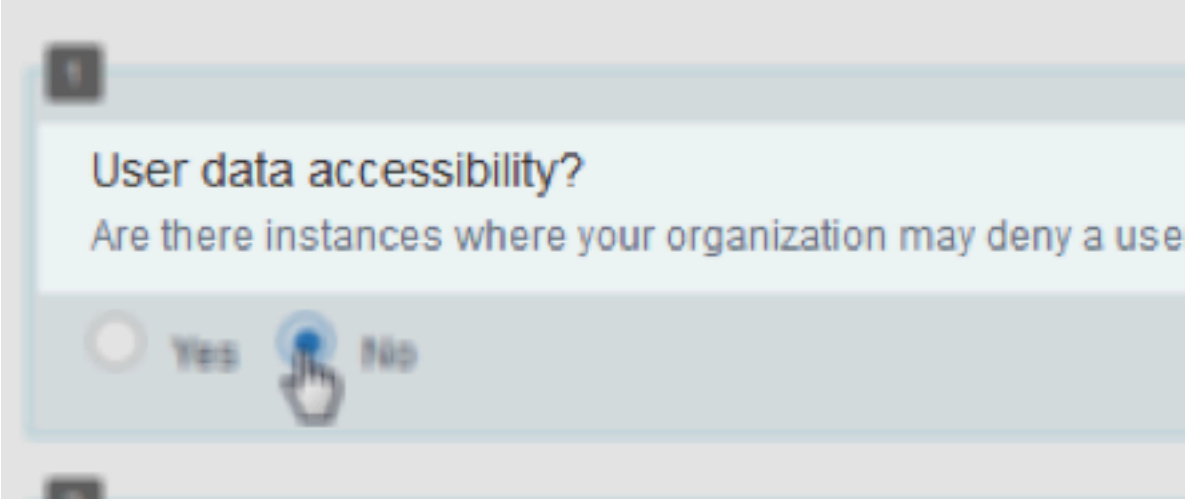
PIA is a team effort requiring input from multiple stakeholders. Work closely with your cross-functional partners and clearly define roles and responsibilities.

If possible, it's valuable to have the privacy office running the PIA effort; however, it is important for corporate governance, risk management, security and other compliance teams to own completion of parts of the PIA process.

What the PIA process must analyze

Answers to PIA questionnaires must analyze and describe several fundamental areas concerning personal data:

- What are the nature and sources of the information we are collecting?
- For what purpose do we collect the personal data elements (e.g., to determine eligibility, for product registration)?
- How do we intend to use the personal data (e.g., to verify existing data, for sales and marketing)?
- Will the personal data be shared with an affiliate or a third-party for a specified purpose?
- Other than required information and authorized uses, do we permit individuals to decline to provide personal data or to consent to particular uses of the data?
- How do individuals grant their consent?
- Which security controls (e.g., log-in credentials, single sign-on, access controls) will we implement to safeguard the personal data?



Other PIA considerations

Budget — Agreeing on budget will help clarify the expenses incurred by the process of conducting PIAs. The expenses include contractor and consulting fees, tools that help automate the assessment process and the opportunity costs of employees spending time away from their principal duties to work on PIAs. Privacy programs can often be underfunded relative to other corporate initiatives, so it is important to plan in advance for PIAs, allocate resources for the unexpected and find areas for efficiency.

Timeframe — Especially in startups and small businesses, employees often launch the assessments with dedication; however, they sometimes must abandon the effort to put out fires or launch other projects. As with the management of any project, it is useful to obtain early commitment on a realistic timeframe from all participants and to schedule regular meetings, depending on the size of the company and the amount of personal information involved. In the fast-paced business landscape of PIA-dependent projects like mergers and acquisitions, the privacy office wants to be viewed as an enabler of change, not as an anchor holding back the rest of the enterprise.

Resources — Finally, it is important to staff the privacy office with an adequate number of suitably skilled employees. The people-factor becomes especially important when the effort requires cross-departmental support, which is critical for quickly identifying data flows and data handling practices.

CONCLUSION

As the possibilities for acquiring and using personal data continue to grow, so does the responsibility for adhering to individuals' privacy choices. To avoid violating laws, standards and policies, companies must now analyze how changes to their products, services, systems and business practices affect personal data.

The PIA process serves as benchmark for evaluating a company's understanding of how it handles personal data. As the PIA team asks detailed questions and analyzes the answers from the business, it alerts stakeholders to potential privacy risks and helps avert regulatory and civil penalties for the improper handling of personal information.

ABOUT TRUSTe

TRUSTe is the leading global Data Privacy Management (DPM) company and powers trust in the data economy by enabling businesses to safely collect and use customer data across their customer, employee, and vendor channels. Our SaaS-based DPM Platform gives users control over all phases of data privacy management from conducting assessments and implementing compliance controls to managing ongoing monitoring. Our Data Privacy Management Services, including assessments and certifications, are delivered by an expert team of privacy professionals. Thousands of companies worldwide rely on TRUSTe to minimize compliance risk and protect their brand.

Images in this paper are taken directly from demo data within TRUSTe Assessment Manager.