

The Ultimate PIA and DPIA Handbook for Privacy Professionals

Everything you need to know to understand, develop, implement, and roll out a GDPR compliant and operationally efficient PIA and DPIA process for your privacy program.

March 22, 2017

Disclaimer

No part of this document may be reproduced in any form without the written permission of the copyright owner.

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. OneTrust LLC shall have no liability for any error or damage of any kind resulting from the use of this document.

OneTrust products, content and materials are for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue. OneTrust materials do not guarantee compliance with applicable laws and regulations.

CONTENTS OF THIS HANDBOOK

Part 1: Understand Requirements and Terminology 4

What is a PIA and a DPIA?..... 4

PIAs and Privacy by Design 5

Is Your PIA Process GDPR Compliant? (10 Step Checklist) 6

Additional GDPR Based Guidance Provided by EU Regulators..... 10

Pre-GDPR Guidance Available as a Reference Point 12

Non-EU: Requirements and Specific Guidance in Other Jurisdictions..... 15

Relevant Industry Standards and Methodologies 15

Part 2: Building the PIA and PTA Questionnaires 17

Creating the PIA/DPIA Questionnaire (10 Steps) 17

Templates Available as Starting Points 23

Part 3: Embedding the PIA within the Organization (10 Step Checklist)..... 25

1. Design the right overall workflow..... 25

2. Select the right tools to implement the PIA process 25

3. Decide the level of automation that makes sense for you 26

4. Identify the right project lifecycle triggers to integrate with for Privacy by Design 26

5. Enable self-service access to the business..... 27

6. Roadmap the technical Integrations with Existing Tools 27

7. Integrate with the Information Security and/or Vendor Assessment Process 28

8. Align with “Agile” Business Processes 28

9. Figure out the staffing for who will review the completed PIA 29

10. Generate valuable reports and metrics..... 29

Reference: Glossary of Terms..... 31

Reference: Risk Assessment Standards and Methodologies 32

Risk Management Frameworks 32

Risk Analysis Frameworks 33

Privacy Risk Management Frameworks 35

About OneTrust..... 37

Part 1: Understand Requirements and Terminology

What is a PIA and a DPIA?

A Privacy Impact Assessment (PIA) is a questionnaire to identify and help reduce privacy risk

Privacy Impact Assessments (PIAs) are fundamental to evaluating an organization's privacy activities, and to mitigating risks as efficiently as possible. PIAs are not only useful, but are oftentimes mandatory for privacy compliance.

Privacy impact assessments can differ greatly in terms of scope, form, ways of being conducted, and even language. Companies across the world assess privacy impacts and potential risks of a project or product at the outset to comply with legal obligations or to ensure the quality of the product or services.

A Data Protection Impact Assessment (DPIA) is a specific type of PIA that is described in the EU GDPR and comes with unique obligations

With the new European General Data Protection Regulation (GDPR)¹ coming into effect on May 25, 2018 companies must go through great changes regarding their privacy program, particularly how they handle their processing of personal data as well as their ability to demonstrate compliance.

Data protection impact assessments (DPIA) are addressed in the GDPR in Article 35, which states: "Where a type of processing in particular using new technologies, and considering the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."²

In addition to Article 35 in GDPR, there are additional articles and recitals in the GDPR that are important to consider when implementing your DPIA process. These specifics are covered specifically in the EU GDPR Requirements section of this handbook.

¹ GDPR available at http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

² Article 35(1)

Common Pitfall: Your PIA is NOT a DPIA - The terminology matters

Some people use the terms PIA and DPIA interchangeably, but there is a notable distinction between the two. The term DPIA is explicitly defined in the GDPR, and includes specific record keeping obligations that are unique. These specific obligations are outlined in this handbook for reference.

Many organizations who have an existing PIA processes in place may be complacent and incorrectly be under the impression that they already meet the DPIA obligations of GDPR. This is a dangerous misconception!

The term DPIA should be reserved and strictly used only when the DPIA triggers in the GDPR are met, and specific care must be taken to record the DPIA in a GDPR compliant format. This format is covered in this handbook as well.

It is for this reason that many organizations choose to implement a workflow that contains an initial “Risk Analysis” or “Threshold” questionnaire that is lightweight and can be performed first to understand the overall risk and determine if a full DPIA is required. This threshold step, described in detail in this handbook, is also beneficial to keep the overall process agile and business friendly.

PIAs and Privacy by Design

A PIA, implemented correctly, can be a way to operationalize Privacy by Design

Privacy by Design was developed by Former Ontario Information and Privacy Commissioner, Ann Cavoukian as an approach to privacy where privacy becomes an organization’s default mode of operation and privacy is integrated into every step of their development processes.³

This means that privacy is embedded into product design and development to make sure the proper choices are available for people using the products, and the default options are the most privacy preserving.

Although Privacy by Design (PbD) was created independently from the GDPR, the GDPR adopts PbD in Article 25.

Article 25 of the EU Data Protection Regulation, includes the concept of “privacy by default” which overlaps heavily with Privacy by Design but not expressly adopt all its principles.

³ Privacy by Design: The 7 Foundational Principles <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>

Article 25 states that “Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.”

The PIA/DPIA is a critical operational and record keeping tool to be able to demonstrate compliance with Article 25. The PIA must be operationalized and embedded into the product lifecycle so that it is triggered during the design process of a product, and the PIA must include the proper set of questions to help the product designers analyze the proper privacy by design principles.

GDPR also requires an organization to keep records of their compliance activities to be able to demonstrate compliance (Article 24) and accountability (Article 5), and the PIA helps meet this obligation by storing the decision-making history and records.

Is Your PIA Process GDPR Compliant? (10 Step Checklist)

Requirements for a DPIA are complex and scattered throughout several articles and recitals

The section below paraphrases and summarizes some of the key articles and recitals in GDPR that impact the requirements, process, documentation, and records for a DPIA.

1. A DPIA is required only when the processing activity is likely to result in high risk to harm to the individual

- **Article 35** is the primary article that outlines the obligations for a “Data Protection Impact Assessment”
- **Article 35 (1)** carry out a DPIA when the processing is likely to result in high risk.
- **Recital 92** “DPIAs broader than a single project”
 - Public authorities or bodies intending to establish common applications, or controllers plan to introduce a common application across industry sector – DPIA may be broader than single project.
- **Recital 93** “public sector requirement”
 - Requirement for member state to carry out DPIA

2. Risk must be analyzed from the view of the data subject, not the business, and include likelihood and severity
 - **Recital 75** describes how risks should be analyzed, including how you may want to consider evidencing in your DPIA how risk was analyzed. Key items to consider include:
 - Risk to the rights and freedoms of natural persons – NOTE: Not business risk, but risk to the data subject
 - Likelihood and Severity
 - Physical, material, or non-material damage
3. The following “high risk” or DPIA triggers must be accounted for
 - **Article 35 (3)** specific cases where a DPIA are required
 - Systematic evaluation of personal aspects based on automated processing, including profiling, and which decisions are based that produce legal effects concerning the natural person or significantly affect them
 - Large scale processing of special categories (mentioned in Article 9(1))
 - Systematic monitoring of publicly accessible areas
 - **Article 35 (11)** review should be conducted when there is a change in risk
 - **Recital 89** Additional examples of processing that may result in high risk that would require a DPIA:
 - Using new technologies
 - New kind of data
 - Necessary considering the time has elapsed since the initial processing
 - **Recital 91** “large-scale processing and automated decision making”
 - High risk may be triggered by large-scale processing operations which aim to process a considerable amount of personal data which could affect many data subjects
 - A new technology is used on a large scale
 - DPIA needed when personal data is used to make decisions following a systematic and extensive evaluation of personal aspects of a natural person
 - Processing special categories of data, biometric data, data on criminal convictions
 - DPIA required for monitoring publicly available area on large scale
 - DPIA NOT needed if processing concerns data from patients or clients by an individual physician, health care professional, or lawyer.

4. Include the additional reference lists being produced by the EU regulators on types of processes that trigger DPIA

- **Article 35 (4)** supervisory authorities will provide guidance on what types of activities require a DPIA
- **Article 35 (5)** supervisory authorities may also provide cases that do NOT need a DPIA

5. Include specific documentation requirements listed in GDPR

- **Article 35 (7)** what should be included in the DPIA
 - a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
 - an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
 - an assessment of the risks to the rights and freedoms of data subjects; and
 - the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with [the GDPR] considering the rights and legitimate interests of data subjects and other persons concerned.
- **Article 35 (8)** codes of conduct from Article 40 should be included in the PIA assessment if applicable
 - Controllers may also be required to “seek the views of data subjects or their representatives on the intended processing” and conduct a prior consultation with the competent supervisory authority⁴.
- **Recital 78** include technical and organizational measures to document as part of the Privacy by Design review portion of a PIA
 - Data minimization
 - Pseudonymizing personal data as soon as possible
 - Transparency regarding the functions and processing of personal data
 - Enabling the data subject to monitor the data processing
 - Enabling the controller to create and improve security features
- **Recital 84** “Processing Operations That Are Likely to Result in a High Risk”
 - A DPIA should include: origin, nature, particularity, and severity of the risk
- **Recital 90** “items to include in impact assessments”
 - Assess the likelihood and severity of the high risk
 - Consider the nature, scope, context, and purpose of processing and sources of risk

⁴ Article 36 of the GDPR

- Measures, safeguards, and mechanisms for mitigating that risk

6. Data Subject views should be reviewed during the DPIA

- **Article 35 (9)** controllers should seek views of data subjects

7. Additional questions should be in a DPIA to demonstrate overall accountability with GDPR

- **Article 5** “Principles Relating to Processing of Personal Data”
 - Article 5 (2) states the controller shall be responsible for, and be able to “demonstrate compliance with, paragraph 1 (‘accountability’)”
 - A PIA can contain records that allows an organization to demonstrate compliance and accountability with the principles of GDPR.
 - This may translate into making sure that the PIA includes questions that map back to each of the principles in Article 5(1)

8. Additional questions should be in a DPIA to operationalize Privacy by Design

- **Article 25** “Data Protection by Design and by Default”
 - A PIA can be the way to demonstrate Privacy by Design. This translates into the following requirements for a PIA:
 - Maintain timestamp evidence showing the PIA is performed at the appropriate time in the project lifecycle
 - Include questions in a PIA that relate to Privacy by Design and Default including items specifically mentioned:
 - Article 25 (1) Technical and organizational measures implemented such as “pseudonymisation” and “data minimization”
 - Article 25 (2) by default, only personal data necessary for each specific purpose of the processing are processed
 - This also mentions that a PIA should separately account for each specific purpose of processing, and minimize data specific to each purpose.

9. Prior Consultations with DPA required when risk cannot be mitigated

- **Article 36** “Prior Consultation”

- Article 36 (1) says that if the DPIA reveals a high risk that cannot be properly mitigated, the supervisory authority (DPA) should be consulted prior to moving forward with the processing.
- Article 36 (2) says the DPA has 8 weeks to reply with written advice, but can be extended by 6 weeks based on the complexity. The supervisory authority may request more information, and in this case, the time limits for them to respond get suspended.
- Article 36 (3) states what should be included in the consultation request
- In practice, it is speculated that this Article relates more to public sector organizations than private sector organizations. Since this is not explicitly mentioned in the GDPR, even privacy sector organizations should be mindful of this obligation. There is much active discussion on how a DPA will provide guidance based on the harm vs. the benefits of the processing, and what would be considered a benefit.

10. The DPO doesn't need to lead the DPIA, but should provide advice during the DPIA

- **Article 35**
 - Article 35 (2) controller should seek the advice of the data protection officer (DPO)
- **Article 39 "Tasks of the Data Protection Officer"**
 - Article 39 (1C) provide advice in the DPIA

Additional GDPR Based Guidance Provided by EU Regulators

Belgian DPA Guidance

As the Belgian DPA (*Commission de la protection de la vie privée*) highlighted in a recent [publication](#), data protection impact assessment (DPIA) obligations under the upcoming [General Data Protection Regulation](#) (GDPR) – particularly as it relates to how companies will be required to conduct them – are still quite nebulous.

To guide companies with implementation, and to answer the many practical questions raised by this new obligation, the Belgian DPA issued a draft recommendation on the subject and launched a public consultation to obtain input and suggestions from stakeholders (controllers, processors, and other concerned persons) before releasing the final recommendation.

Comments could be filed with the Commission until 28 February 2017. The Article 29 Working Party and ENISA (European Union Agency for Network and Information Security) are also expected to release additional guidance on this point in the near future.

The draft recommendation provides some insight about the legal context that gave rise to this new DPIA obligation, namely the accountability principle and the risk-based approach, both included in the GDPR.

Under the [Directive 1995/46/EC](#), controllers had a general obligation to notify their local data protection authority of any processing. This obligation created severe administrative and financial burden without improving data protection rights for individuals.

DPIAs were introduced to resolve this issue, and are now relied upon to assess risks to the rights and freedoms of natural persons which may occur through processing of personal data, as well as consider and determine how such risks can be avoided.

The key takeaways from the Belgian recommendation are the following:

1. The essential elements of a DPIA
2. The circumstances under which DPIAs are required
3. The circumstances under which a prior consultation with the competent supervisory authority is required, and
4. The stakeholders who should be involved in the DPIA
5. The two lists that will help to determine whether a DPIA is necessary

Under the GDPR, each supervisory authority is tasked with establishing a public a list of the kind of processing operations that are subject to the requirement for a DPIA [1].

The Belgian draft recommendation sets forth such a list, which includes twelve specific situations, most notably: processing activity that uses biometrics or genetic data to identify individuals, and processing activity that establishes large-scale profiling on individuals.

Additionally, each supervisory authority *may* establish and make public a list of the kind of processing operations for which no DPIA is required [2].

The Belgian draft recommendation presents this list, as well, which includes seven specific situations, most notably: processing activity that concerns the accounting of the controller (where data is exclusively used for this purpose), and processing activity that concerns data that's critical for processing, data that's kept for longer than needed, and data that's shared with third parties, but only where necessary.

The recommendation emphasizes, however, that the lists are non-exhaustive, and should be used as starting points for controllers when assessing the necessity to conduct a DPIA.

It also stresses that the lists do not, in any way, impact the obligation for controllers to implement appropriate technical and organizational measures to ensure and to demonstrate that the processing is performed in accordance with the GDPR, considering the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons [3].

Furthermore, the recommendation indicates that it clearly results from Article 36 (1) that a prior consultation with the supervisory authority is only needed where the residual risk is high; only where the considered processing would present a high risk if the controller did not take any efficient measures to mitigate the risks.

The full draft recommendation can be accessed in [French](#) and in [Dutch](#).

[1] Article 35(4) of the GDPR

[2] Article 35(5) of the GDPR

[3] Article 24(1) of the GDPR

Article 29 Working Party Guidance

As of the publishing of this guide, the Article 29 Working Party is still finalizing their official guidance. Contact OneTrust at support@onetrust.com for an up-to-date version of this handbook that includes the latest guidance.

Additional Guidance Expected

Additional guidance from various member states is expected soon. Contact OneTrust at support@onetrust.com for an up to date version of this handbook that includes the latest guidance.

Pre-GDPR Guidance Available as a Reference Point

CNIL (France) - Privacy Impact Assessment (PIA) Methodology, Tools, and Good Practices

- Methodology: <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf>
- Tools: <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf>
- Good Practices: <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-3-GoodPractices.pdf>

The CNIL offers three documents that expertly lay out the PIA process and the necessary legal and operational requirements.

Methodology

“A PIA rests on two pillars:

1. fundamental principles and rights, which are “non-negotiable”, established by law and which must be respected and cannot be subject to any variation, regardless of the nature, severity, and likelihood of risks;

2. management of data subjects' privacy risks, which determines the appropriate technical and organizational controls to protect personal data.⁵

Tools

To implement those two pillars, the approach consists of 4 steps:

1. Context study
 - a. Define and describe the processing(s) of personal data under consideration, its (their) context and stakes;
2. Controls study
 - a. Identify existing or planned controls (those to fulfill the legal requirements, and those to treat the privacy risks);
3. Risks study
 - a. Assess the risks that are related to the security of data and that could have impacts on individuals' privacy, to check if risks have been treated adequately;
4. Validation
 - a. Decide whether to accept the manner in which it is planned to fulfill legal requirements and to treat risks, or to reiterate the previous steps.

Good Practices

This document is "a catalogue of good practices intended to treat risks that the processing of personal data may pose to the civil liberties and privacy of data subjects." Risks discovered in PIA must be matched up with proper controls before a decision can be made to decide whether to move forward. The catalogue helps to determine the measures proportionate to the risks identified.

UK Information Commissioner's Office: Privacy Impact Assessment Code of Practice

- Available: [Privacy Impact Assessment Code of Practice](#)

Published in February of 2014 by the Information Commissioners Office (ICO) this is a code of practice for conducting PIA. It replaces the ICO's earlier work, the Privacy Impact Handbook, which was last updated in 2009 and was one of the early comprehensive documents to describe the PIA process in detail. The focus of the code is on minimizing harm caused by use or misuse of personal data. The code is organized into the following chapters:

- "Chapter 1 - Introduction to PIAs"

⁵ French Commission Nationale de l'Informatique et des Libertés: Privacy Impact Assessment (PIA) Methodology page 4 of 19 <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf>

- Chapter 2 - The PIA process
- Chapter 3 – Consultation
- Chapter 4 – Identifying the need for a PIA
- Chapter 5 - Describing information flows
- Chapter 6 - Identifying privacy and related risks
- Chapter 7 - Identifying and evaluating privacy solutions
- Chapter 8 – signing off and recording the PIA outcomes
- Chapter 9 – Integrating PIA outcomes back in to the project plan”

The code is particularly useful in highlighting projects that might require a PIA and provides a list:

- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more organizations seek to pool or link sets of personal data.
- A proposal to identify people in a group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding Automatic number plate recognition capabilities to existing CCTV).
- A new database which consolidates information held by separate parts of an organization.
- Legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring.⁶⁷”

Additionally, the code sets out a suggested process for PIAs:

- “Identify the need for a PIA
- Describe the information flows
- Identify the privacy and related risks
- Identify and evaluate the privacy solutions
- Sign off and record the PIA outcomes
- Integrate the outcomes into the project plan
- Consult with internal and external stakeholders as needed throughout the process⁸”

⁷ Conducting privacy impact assessments code of practice (ICO) 20140225 page 9 <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>

⁸ Conducting privacy impact assessments code of practice (ICO) 20140225 page 11 <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>

It's also worth noting that starting on page 25 the code includes lists of individual, corporate, and compliance risks that should be considered. Overall, the document is well written and important background reading to understanding the expectations surrounding PIAs.

Non-EU: Requirements and Specific Guidance in Other Jurisdictions

Canada

- <https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/>

Hong Kong

- https://www.pcpd.org.hk/english/resources_centre/publications/books/files/publication.pdf
- https://www.pcpd.org.hk/english/resources_centre/publications/books/files/publication.pdf
- https://www.pcpd.org.hk/english/resources_centre/publications/files/InfoLeaflet_PIA_ENG_web.pdf
- <https://privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment/>

New Zealand

- <https://privacy.org.nz/assets/Files/Guidance/Privacy-Impact-Assessment-Part-2-FA.pdf>
- <https://privacy.org.nz/assets/Files/Guidance/Privacy-Impact-Part-1.pdf>
- <https://privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment/>
- <https://privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment-handbook/>

USA S.E.C.

- <https://www.sec.gov/about/privacy/piaguide.pdf>

Relevant Industry Standards and Methodologies

In addition to regulatory guidance, several industry standards for risk assessments exist that provide a framework for conducting PIAs. A sample of these frameworks is listed here, and additional detail around them is provided in the reference section of this document.

- ISO 31000:2009 Risk management — Principles and guidelines
- European Network and Information Security Agency (ENISA): Risk Management
- Expression des Besoins et Identifications des Objectifs de Sécurité (EBIOS)
- Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)
- ISO 27005: Security Risk Assessment
- NIST SP 800-30 Guide for Conducting Risk Assessments
- ISO/IEC 29100:2011 Information technology — Security techniques
- NIST SP 800-122, Guide to Protecting the Confidentiality of PII
- Under Development: IEE P7002 - Data Privacy Process

Part 2: Building the PIA and PTA Questionnaires

Creating the PIA/DPIA Questionnaire (10 Steps)

1. Incorporate the required GDPR or other regulatory requirements

Part 1 of this handbook reviewed in depth the record keeping requirements in GDPR, as well as summarized other jurisdiction guidance available. One of the most common pitfalls of a PIA process is that so much work is being done, however, some of the specific regulatory record keeping requirements are neglected so the organization is still not able to demonstrate accountability. Below is a summary checklist of items to remember when designing your questionnaire for GDPR, this can be used as a rough framework to review with your legal counsel.

Description and Scope

When assessing whether a Data Protection Impact Assessment meets requirements, start with the requirements in Article 35(7) and then dig deeper with the additional citations listed below. Article 35(7) requires (in part) that the assessment shall contain at least: “(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;”

- ✓ Description
 - CNIL PIA 2 tools (General description)
- ✓ Purpose
 - GDPR Rec.39, 40, 41; Art.6(1)
- ✓ Benefit Question
 - CNIL PIA 2 tools (Stakes of the processing to be described in the General description of the PIA).
- ✓ Personal Data
 - GDPR Article 4(1) "Personal data"
 - Article 9 GDPR (processing of special categories of data)
- ✓ Harm
 - Recital 75 of the GDPR

Processing

Again, returning to the requirements in Article 35(7) ensure that the PIA contains “(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;”

- ✓ Minimization
 - GDPR Art. 5(1)(c)
- ✓ Accuracy
 - GDPR Art. 5(1)(d)
- ✓ Retention
 - GDPR Art. 5(1)(e)
- ✓ Basis for Processing
 - GDPR Art. 5(1)(a) Lawfulness of Processing, Art. 6

Data Subject Rights

Furthermore, the requirements in Article 35(7) insist that the PIA contains (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1. This means that the PIA considers the nature, scope, context, and purposes of the processing that is likely to result in a high risk to the rights and freedoms of people. While not essential, it might make sense to take a broader approach, as shown below, to review the rights of data subjects more fully to not only manage high risks but ensure that assessed projects enable certain data subject rights that are best addressed when the design process is still flexible and mechanisms for enabling these rights can be incorporated as requirements.

- ✓ Right to Information
 - GDPR Rec.58, 60; Art.13-14
- ✓ Right to Object
 - GDPR Rec.50, 59, 69-70, 73; Art.21
- ✓ Right of Access
 - GDPR Rec.63; Art.15
- ✓ Right to Rectification
 - GDPR Rec.39, 59, 65, 73; Art.5(1)(d), 16
- ✓ Right to Data Portability
 - GDPR Rec.68, 73; Art.20
- ✓ Right to Erasure
 - GDPR Rec.65-66, 68; Art.17
- ✓ Right to Restrict Processing
 - GDPR Rec.67; Art.18

Measures to Address Risk

Article 35(7) requires the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data. Article 25 requires appropriate

technical and organizational measures, acting as necessary safeguards to meet the requirements of this Regulation and protect the rights of data subjects.

- ✓ Recording of the risks, controls, and decision
 - CNIL PIA 1 Methodology & 2 tools

Transfers (Optional)

Assessing a project for risk via a PIA can also be a good time to assess whether cross border transfers are present and are being addressed correctly. There are only so many times that the privacy team can ask questions and collect information so this is a good time to learn more.

- ✓ Transfer Mechanisms/Controls
 - GDPR Rec. 103-107 & 169 Art. 45

2. Incorporate Article 30 Processing Records Requirements

In addition to the GDPR components in item 1, many organizations also choose to include the specific record keeping requirements from Article 30 in the GDPR into their questionnaire as well.

Most organizations who have a GDPR based privacy program use Article 30 as the foundation of their data mapping initiative.

By incorporating the same set of questions from the data map into the PIA questionnaire, the PIA results can be fed back into the data map to keep it up to date and evergreen. Automation tools, such as OneTrust, can automate this evergreen process as well.

3. Organize the questions in an overall framework

Once these questions from the above have been compiled, it is important to add some structure and organization to the questionnaire. Below are two example ways of structuring and organizing the questionnaire.

Example 1:

1. Notice
2. Choice, Consent & Legitimate Processing
3. External Transfers & Sharing
4. Access & Other rights of the employee
5. Security
6. Integrity, quality & data migration
7. Governance, Policy, and Training
8. Sensitive & Special Categories

Example 2:

1. System Information
2. Contact Information
3. Data Lifecycle
 - b. Data attributes collected
 - c. Collection mechanism
 - d. Consent and Notification process
 - e. Usage
 - f. Transfers
 - g. Disclosure to other parties
 - h. Storage
 - i. Destruction
 - i. Mapping to principles (HIPPA, GDPR, etc.)

4. Re-word the questions in a business-friendly way

Much of the terminology familiar to legal or privacy professionals may be foreign to business users. Be sure to re-word and continue to test the questions to avoid frustration from the business.

Example:

“What is the purpose for processing?”

Vs.

“What is the business reason for using this data”

5. Embed training and support

Ease-of-use is essential for getting accurate responses. When possible include additional descriptions and tips that can be revealed at the time the respondent is reviewing the question. There is a good chance that a confused respondent will provide poor quality responses and the privacy team is only as effective as the information they must work with.

6. Add conditional skip questions

PIAs are all about getting the right questions to the right people, and the fewest number of right questions to those people.

When designing your PIA questionnaire, it is a best practice to build in question skip logic or branching logic rules so that questions that are not applicable to a specific project do not need to be presented to the business user.

7. Allow for flexible responses

Don't force respondents to submit the wrong answer! Respondents may not have all the answers to your privacy questions, and should be given the option to choose "Not Sure" or "Other," which allows them to fill in any additional detail they can share. These options invite a conversation with the privacy team that often reveals key details that would have been left out.

8. Incorporate a freeform text box

Structured responses are incredibly important. Yes or no, A or B, these are answers that can be connected to conditional logic and used to enhance automation. They also allow for comparative analyses. That said, in many cases, structured responses should not be the only response. In many causes you will want to ask respondents to explain their answer. This allows respondents can offer additional comments or provide explanations for complicated matters. Offering both structured and unstructured answers to a question allows the privacy team to get the best of both worlds, great automation along with context and detail.

9. Create an integrated "Threshold" Step

They go by many names: Gateway, Threshold, Pre-PIA, Screening, Risk Assessment, etc.

Regardless what you call it, having a threshold step is critical to keep your PIA process agile and usable in a business environment.

Avoid PIA fatigue within your organization. Threshold assessments are the brief screen questions that can be asked to determine whether risk is present and more information is needed. Always remember that the PIA process may be the only interaction that the privacy has had and possibly will have with individuals within an organization and it's important to put your best foot forward. The PIA experience and the individuals experience of what it is like to work with the privacy team. It's important the privacy team gets what it needs and doesn't waste anyone's time. Anything longer than 10 questions is too much for a threshold. Short and simple works best.

DPIA under the GDPR can be approached as a two-step requirement by incorporating this threshold:

- Step 1: A privacy threshold assessment or simple privacy impact assessment which would aim to determine whether a processing activity is likely to result in high risks to the rights and freedoms of data subjects

- Companies should incorporate in their PIA the elements set out in Recital 75 of the GDPR⁹
- Step 2: When (and only when) the PIA, after the risk review and mitigation phase, suggests that there is still a likelihood of high risks to the rights and freedoms of the data subjects, controller should then conduct a more thorough “Article 35 DPIA”, which should contemplate all the elements mentioned above.

As reflected in this provision, the first challenge for companies is to determine when and whether an “Article 35 DPIA” is required. Moreover, the language of the provision itself¹⁰ suggests that some type of privacy threshold assessment would in fact be necessary prior to the (full) DPIA for the controller to determine first if the type of processing activity that is being considered is indeed likely to result in a high risk, which would then mean that the controller has to conduct the “Article 35 DPIA”.

The GDPR sets out three situations in which the controller is obligated to conduct an “Article 35 DPIA”¹¹:

- (1) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- (2) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; and
- (3) a systematic monitoring of a publicly accessible area on a large scale.

⁹ The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analyzing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

¹⁰ “where a type of processing (...) is likely to result in a high risk (...), the controller shall, prior to the processing, carry out an assessment of the impact”

¹¹ Article 35(3)

Additionally, under the GDPR, each supervisory authority is tasked with establishing a public list of the kind of processing operations that are subject to the requirement for a DPIA¹², and *may* establish and make public a list of the kind of processing operations for which no DPIA is required¹³. The Belgian Supervisory Authority recently issued a draft recommendation on DPIA¹⁴ in which it proposed such lists. Under its draft publication (which was submitted for public comments), controllers shall be required to conduct a DPIA in twelve specific situations, most notably: processing activity that uses biometrics or genetic data to identify individuals, and processing activity that establishes large-scale profiling on individuals. The recommendation also set forth the list of processing activities which should not require a DPIA, including seven specific situations, most notably: processing activity that concerns the accounting of the controller (where data is exclusively used for this purpose), and processing activity that concerns data that's critical for processing, data that's kept for longer than needed, and data that's shared with third parties, but only where necessary.

These triggers can be built into the Threshold questionnaire.

10. Do not ask "Do you collect personal data?"

Privacy professionals talk about personal data all the time. Whether something is or is not personal data is incredibly important and drives the decisions within the privacy team. Other individuals within the organization do not have this focus on personal data and the word does not hold the same meaning for them. A customer study showed that when people were asked "Do you collect personal data?" 30% of people respond "No." Upon follow up, 90% of those that answered "No" should have answered "Yes."

The good news is that it's not hard to get accurate information about whether personal data is being collected. Ask: "*What* data do you collect?" and provide multiple choice selections (i.e. name, phone number, address, etc.) and then other or none of the above. This shows individuals the definition and it can also lead to interesting information being submitted via the "other" field that the privacy team would not have had a chance to review.

Templates Available as Starting Points

OneTrust provides many different types of PIA, DPIA, and Threshold templates.

These templates include conditional logic rules, embedded help and training, and have been created by privacy experts around the world.

¹² Article 35(4)

¹³ Article 35(5)

¹⁴ Available in French at <https://www.privacycommission.be/fr/consultation-publique-sur-la-recommandation-concernant-lanalyse-dimpact-relative-a-la-protection>

Contact OneTrust at support@onetrust.com for access to these templates.

Part 3: Embedding the PIA within the Organization (10 Step Checklist)

1. Design the right overall workflow

There are many potential workflows that can be successful in a PIA process. One of the most common workflows is as follows:

- Business user or privacy office initiates a new project
- Threshold questionnaire gets distributed to the project owner
- Completed threshold questionnaire gets analyzed to determine if a full PIA or DPIA is required
- Full PIA distributed to the project owner, completed and submitted back
- The Privacy Office records risks and recommendations
- Mitigation activities are tracked and followed up on

2. Select the right tools to implement the PIA process

The workflows associated with a robust PIA or DPIA process can become drastically simpler and more automated when using the appropriate tool. Below are some types of tools available:

Free Tools

IAPP | OneTrust Free PIA Platform

IAPP and OneTrust offer a free PIA platform available. Sign up now at [OneTrust.com](https://www.onetrust.com)

Microsoft Templates in Word or Excel

Templates can be created in Word or Excel as an easy way to get started. Although not a suggested long term approach, this can be a great way to finalize and prototype the questionnaires and wording.

Homegrown tools in SharePoint or Workflow Tools

Some organizations choose to re-purpose existing tools for PIA / DPIA processes. It's important to review your implementation of your homegrown solution with the checklists and best practices in this document.

Paid Tools

OneTrust Enterprise Grade Privacy Management Software

OneTrust makes the leading enterprise grade platform comprehensive for privacy programs, including PIA/DPIA activities. The solution is available to be installed in your data center, or in a cloud environment managed by OneTrust. Learn more at [OneTrust.com](https://www.onetrust.com)

GRC – Governance, Risk, Compliance Tools

Many organizations may have an existing GRC tool they use for other compliance activities. Due to the complex requirements, unique record keeping, and business facing collaborative user experience required in privacy management – organizations typically choose to leverage a privacy management solution such as OneTrust, and integrate the solution into the GRC tool rather than attempting to re-built and keep up to date all the privacy tasks themselves in the GRC.

3. **Decide the level of automation that makes sense for you**

There is no privacy team that has a bigger team than they need or more resources than they know what to do with. Manually administering PIAs is time-consuming and time is wasted filling out the PIAs and assessing them. Worse yet, lack of automation also means lack of consistency in storage and follow up which can mean a lack of accountability down the road when it turns out that the risks that were revealed by the assessments were never addressed or were only partially addressed. The more you can automate this process, the more likely your respondents are to participate and the most likely the privacy team will be able to carry out its work effectively by focusing on what matters.

There are different levels of automation available, and not all levels are appropriate for all organizations:

- Workflow automation: automation the distribution and collaboration of the PIA process
- Full threshold automation: fully automate the threshold step to not require any admin intervention or review if low risk processing is detected
- Full PIA automation: fully automate the entire process with a robust set of rules engine that is monitored and audited regularly.

4. **Identify the right project lifecycle triggers to integrate with for Privacy by Design**

Different business teams have different ways they project manage their work. The key is to go one at a time to each business team, understand their project management cycle, and find the appropriate way to integrate into that function. Below are some examples:

- IT Teams sometimes follow a ITIL project management process that includes various review toll gates and security architecture reviews. These toll gates are a great opportunity to insert your PIA process.
- R&D Engineering teams sometimes follow a release process or a SDLC (System Development Lifecycle) process that also includes toll gates and checkpoints that can be integrated with.
- Procurement is another opportunity to insert your PIA process if your organization has a central procurement function.
- Finance Approval – many privacy programs have found success in “following the money”. If you can identify how projects are funded, you can insert yourself into the funding process of that project.

5. Enable self-service access to the business

Once you have identified the right roll gate to insert your PIA process – you can mature the process further by removing the requirement for a privacy team member to manually send a questionnaire to the business.

A self-service portal can be enabled where the business can access the privacy review information themselves.

6. Roadmap the technical Integrations with Existing Tools

Having to log-in to a separate portal, or remember which intranet site to go to in order to conduct a privacy review opens room for error and missed process.

The most effective privacy programs go beyond administrative/operational integrations into business processes and integrate at a more technical level to make privacy a reflex of the activities that business teams are already doing.

For example:

- SharePoint – many business teams have their home base as SharePoint, and your PIA process can be inserted as a link into a team’s existing SharePoint site rather than being a separate portal to log into.
- JIRA – many R&D engineering teams use a tool called JIRA that is essentially a to-do list for developers. Integrating into this tool to help developers track their follow up remediation tasks and feature requests can be the most highly effective way to integrate PbD into engineering teams.
- GRC – some compliance teams already produce questionnaires to business users using an existing GRC tool like RSA Archer. Integrating your PIA tool into the GRC can be an effective way to consolidate these questionnaires.

- Service Now and other ITSM Tools – Some IT teams operate off service management tools like Service Now or BMC Remedy. The PIA process can integrate into this tool to create tickets and follow up tasks for the identified stakeholders who use these tools, typically in IT.

OneTrust provides integration capabilities with these tools, and many others as well, to simplify the integration tasks.

7. Integrate with the Information Security and/or Vendor Assessment Process

There are very few initiatives within an organization that only affect one team/group. For example, when a new feature is being released there is often a privacy and security assessment that needs to take place. Make sure to gather information about other assessments that are taking place around the company and see where the privacy team might be able to work well with others. Try using a threshold assessment that triggers full privacy or security impact assessments. This will present respondents with less work and it will lead to a more effective and integrated approach to managing risk. When it's not clear where integration could happen at an organization, the best place to start is with a conversation with privacy champions to find out what is really happening and where integration can occur.

8. Align with “Agile” Business Processes

Agile or SCRUM is a project management methodology common in R&D organizations, and becoming more popular with other business groups as well.

Sometimes PIA's are at odds with Agile processes that preach operating in short 1 to 2 week “sprints” to complete works, avoiding over planning or over engineering, and reducing the amount of documentation required.

A few ways to integrate into an agile environment include:

- Implementing a lightweight threshold step that can be completed as part of a sprint task
- Integrate directly with the Agile tool to track tasks, such as in JIRA
- Have follow up items identified from the PIA integrated in various sprints
- Use a tool such as OneTrust to reduce the documentation effort required by the business team
- Make sure the PIA process and tool is mobile responsive so individuals can complete PIA or Threshold on the go

9. Figure out the staffing for who will review the completed PIA

Many organizations turn to a concept called “Privacy Champions” to help scale the processes of reviewing the PIA. Sometimes Privacy Champions are called:

- Privacy Advisors
- Privacy Champions
- Privacy Account Managers
- Privacy Angels
- Privacy Gurus
- Privacy Network
- Etc.

The role and function of the privacy champions vary drastically. Most commonly these are business users who either are tapped or volunteer to become knowledgeable in privacy.

The privacy champions can be on point for helping their business teams complete the PIA, can be the first line of defense for answering FAQs, and can also be inserted as reviewers of the completed PIAs.

10. Generate valuable reports and metrics

Reports and metrics are key to a successful program – and different stakeholders may require different views.

Project Managers

- Status reporting on PIAs to understand outliers and lingering tasks
- Time breakdown reporting to understand where the most time consuming parts of a PIA are to optimize

Privacy Compliance

- View of outstanding risks and unmitigated items
- Team utilization reporting

Executive Reporting

- Simple compliance metrics
- Visual representations of data flows
- Trends of risks
- Financial metrics on % of project budget spent on privacy reviews

Regulators

- Reports for DPA consultations
- PbD reports
- Ability to demonstrate compliance for a project

Accuracy tracking and change management reports

- There are many reasons why someone would be uncertain about their questionnaire responses. One reason might be that the question is not clear. Analyzing answer changes on a per question basis across multiple projects will give you insight into the quality of your questions and lead to iterative improvements. Another reason for answer changes might be respondent confusion because of the complexity of the project or a misunderstanding about what is being asked. Respondent confusion can lead to unhappy respondents and inaccurate information. Combat this by tracking any changes to their answers, which can identify reasoning for their hesitation.

Reference: Glossary of Terms

Term	Definition
Data Protection Impact Assessment (DPIA)	A systematic effort to identify privacy risks, foresee problems and bring forward solutions as outlined in the GDPR
Privacy Impact Assessment (PIA)	A questionnaire to analyze the privacy risk of a project.
General Data Protection Regulation (GDPR)	A Regulation by which the European Commission intends to strengthen and unify data protection for individuals within the EU, and address export of personal data outside the EU
CPO	Chief Privacy Officer
DPO	Data Protection Officer
HIPAA	U.S. law passed to create national standards for electronic healthcare transactions
Inherent risk	Risk that an activity would pose if no controls or other mitigating factors were in place; gross risk
Residual Risk	Risk that remains after controls are considered
Pre-PIA	Alternative term for a threshold; a short assessment used to determine the need for a full PIA
Threshold	An assessment used to determine whether a full PIA should be conducted
DPA	Data Protection Authority

Reference: Risk Assessment Standards and Methodologies

Risk Management Frameworks

ISO 31000:2009 Risk management — Principles and guidelines

Available: <https://www.iso.org/obp/ui/#iso:std:43170:en>

This standard provides is not focused on privacy risk, but rather risk in general. Implementation of the standard involves the entire management system and supports the design, implementation, maintenance, and improvement of risk management processes.¹⁵ One area where this standard is useful within the PIA context is risk treatment. Retaining, avoiding, reducing, and sharing the risk(s) and preparing and implementing risk treatment plans is an essential step in the PIA process and following a standard for risk management, such as 31000:2009 an assist with operational efficiency, governance, and organizational confidence in the process. A revision of 31000 is underway with the goal of continuing to simplify the approach.

European Network and Information Security Agency (ENISA): Risk Management

Available: <http://www.enisa.europa.eu/activities/risk-management>

The European Union Agency for Network and Information Security (ENISA) is a center of expertise for cyber security in Europe. The Agency works closely together with Members States and the private sector to deliver network and information security advice and solutions. ENISA's risk management methodology is outlined in the first 38 pages of the 168-page report with the remainder of including an extensive inventory of other risk management methods and tools.¹⁶

¹⁵ <https://www.iso.org/iso-31000-risk-management.html>

¹⁶ European Network and Information Security Agency (ENISA), Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools, Heraklion, June 2006.

<http://www.enisa.europa.eu/activities/risk-management>

The ENISA risk management methodology works well as a way of implementing a PIA and it addresses integration of its risk management methodology with other processes in the organization. ENISA makes a distinction between existing and emerging risks. Existing risks using a standard risk management approach and emerging risk require additional intention and process.

Risk Analysis Frameworks

Expression des Besoins et Identifications des Objectifs de Sécurité (EBIOS)

Available: <https://www.ssi.gouv.fr/uploads/2011/10/EBIOS-1-GuideMethodologique-2010-01-25.pdf>

EBIOS is a high-level method for risk management. Its method mainly addresses information security but it can be leveraged to address other types of risk. EBIOS is mainly used in France, where it is recommended for use in the government as well as private companies working with the government. Compatibility with other information security management and risk management including: ISO 27001, ISO 27005, ISO Guide 73, and ISO 31000.

EBIOS views risk as a combination of:

- threat source,
- threat,
- vulnerability,
- impact.

EBIOS is not a great risk analysis methodology for companies looking to build a large multijurisdictional program but the method works well in France and it also is an excellent reference for those that are looking for some additional context and background on risk analysis.

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

Available: <https://www.cert.org/archive/pdf/01tr016.pdf>

In 1999, Carnegie Mellon University published OCTAVE via the Software Engineering Institute¹⁷. The OCTAVE method is not a full risk management method but rather a risk evaluation method. For companies looking for a point in time analysis this can be a useful approach. Because this is not a full

¹⁷ Alberts, Christopher J., and Audrey J. Dorofee, OCTAVESM Criteria, Version 2.0, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 2001. <https://www.cert.org/archive/pdf/01tr016.pdf>

“Plan-Do-Check-Act” approach it is not a perfect fit for adopting in conjunction with PIAs but is helpful in developing structure around risk analysis

ISO 27005: Security Risk Assessment

Available <https://www.iso.org/standard/56742.html>

ISO 27005 is standard for information security risk management details an ongoing process for examining the external and internal context, identification, and assessment of risks, and then recommending how to address those risks.¹⁸ ISO 27005 is aligned with the risk management standard ISO31000, which makes it easy to integrate Enterprise Risk Management with information security risk management. Additionally, ISO27005 uses the concepts in common with ISO 27001 and ISO 27002 which provides an effective framework for information security management. PIAs fit well into the ISO 27005 process where risk identification and the application of appropriate controls is carried out.

NIST SP 800-30 Guide for Conducting Risk Assessments

Available: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>

As the standard states in the introduction, “The purpose of risk assessments is to inform decision makers and support risk responses by identifying:

1. relevant threats to organizations or threats directed through organizations against other organizations;
2. vulnerabilities both internal and external to organizations;
3. impact (i.e., harm) to organizations that may occur given the potential for threats exploiting vulnerabilities; and
4. likelihood that harm will occur.”¹⁹

This standard is security focused but the assessment of risk can be helpful in in a PIA context if a focus on privacy is introduced when developing an organizational program. Without that introduction of privacy focus, harms to individuals whose personal data are processed will not be addressed and this will not be an adequate approach.

¹⁸ International Organization for Standardization (ISO), Information technology – Security techniques – Information security risk management, ISO/IEC 27005:2011 <https://www.iso.org/standard/56742.html>

¹⁹ NIST SP 800-30 Guide for Conducting Risk Assessments, page 1 available at: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>

Privacy Risk Management Frameworks

ISO/IEC 29100:2011 Information technology — Security techniques

Available: <https://www.iso.org/standard/45123.html>

Standard provides the principles and guidelines for managing, systematically and transparently, any form of risk.²⁰ The standard consists of five main chapters: scope, terms and definitions, principles, framework, and process. As it states on the introduction to the standard:

“The privacy framework is intended to help organizations define their privacy safeguarding requirements related to PII within an ICT environment by:

1. specifying a common privacy terminology;
2. defining the actors and their roles in processing PII;
3. describing privacy safeguarding requirements; and
4. referencing known privacy principles.²¹”

This standard is a popular risk management methodology but because it is a generic risk management methodology, it does not address all the issues that should be covered for a PIA.

NIST SP 800-122, Guide to Protecting the Confidentiality of PII

Available: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf>

NIST 800-122 covers the process and requirements for PIAs adequately address confidentiality risks and applying appropriate safeguards. Whether personal data is processed is an important determination and the standard suggests using a “privacy threshold analyses” (PTAs), also known as “initial privacy assessments” (IPAs) to make this determination. If the PTA concludes that personal data is involved, it triggers a PIA. Another helpful aspect of this standard is the descriptions of safeguard and controls.

In section 4.2.2 topics that are commonly addressed by a PIA are outlined:

1. “What information is to be collected
2. Why the information is being collected
3. The intended use of the information

²⁰ International Organization for Standardization (ISO), Risk management – Principles and guidelines, ISO 31000:2009, Geneva, 15 Nov 2009 <https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en>

²¹ <https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en>

4. With whom the information will be shared
5. How the information will be secured
6. What choices the agency made regarding an IT system or collection of information as a result of performing the PIA performing the PIA.”

While NIST 800-122 is US-centric – and therefore not a great fit when solely relied upon for meeting GDPR DPIA requirements – it is an excellent guide to protecting personal data through the usage of PIAs.

Under Development: IEE P7002 - Data Privacy Process

Available: <https://standards.ieee.org/develop/project/7002.html>

This is a new standard that is under development. The first meeting of the working group was in March, 2017. As the Personal Data Privacy Working States (<https://standards.ieee.org/develop/project/7002.html>) “The purpose of this standard is to have one overall methodological approach that specifies practices to manage privacy issues within the systems/software engineering life cycle processes. This standard defines requirements for a systems/software engineering process for privacy oriented considerations regarding products, services, and systems utilizing employee, customer, or other external user's personal data. It extends across the life cycle from policy through development, quality assurance, and value realization. It includes a use case and data model (including metadata). It applies to organizations and projects that are developing and deploying products, systems, processes, and applications that involve personal information. By providing specific procedures, diagrams, and checklists, users of this standard will be able to perform a conformity assessment on their specific privacy practices. Privacy impact assessments (PIAs) are described as a tool for both identifying where privacy controls and measures are needed and for confirming they are in place.”

About OneTrust

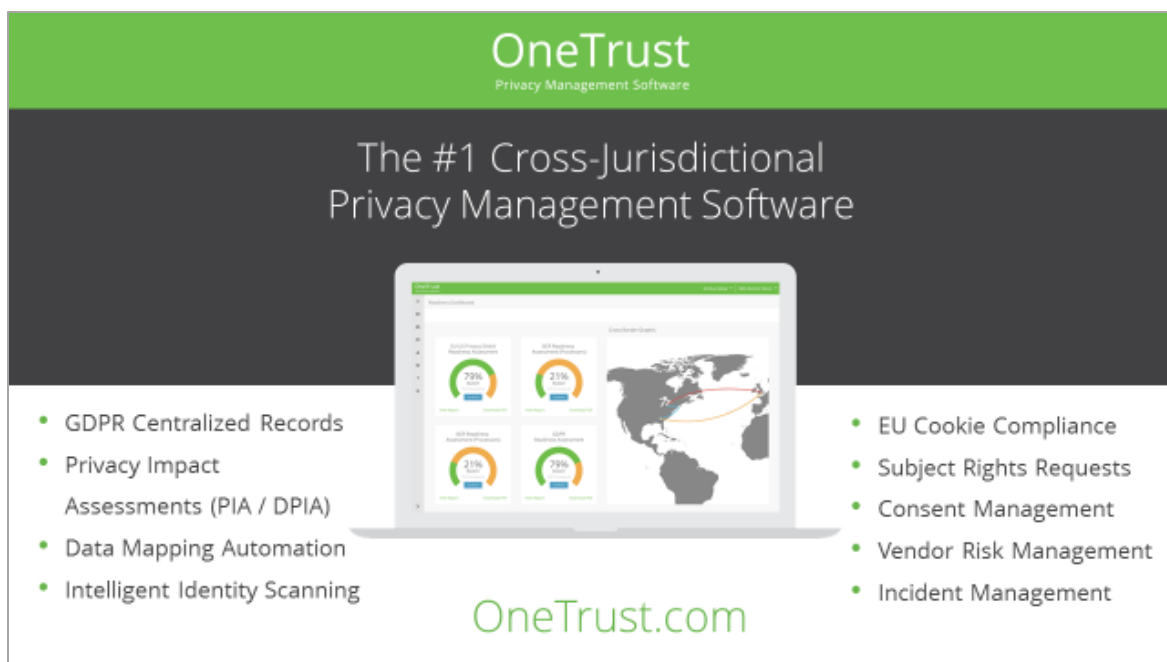
OneTrust is the leading and fastest growing privacy management software platform used by over 1,000 organizations globally to comply with data privacy regulations across sectors and jurisdictions, including the EU GDPR and Privacy Shield.

Our comprehensive, integrated, technology-based solutions include readiness and privacy impact assessments, data inventory and mapping, automated identity and data discovery, website scanning and cookie consent management, subject rights and consent management, incident reporting, and vendor risk management.

The OneTrust platform is pre-configured with templates and workflows that can be easily tailored via our point-and-click UI based on unique industry and organizational requirements. We make it easy for privacy teams to get started with OneTrust by giving them the flexibility to upgrade platform capabilities as their program matures, deploy in the cloud or on premise, and scale to support a growing network of privacy champions.

OneTrust is based in Atlanta, GA and London, UK with a team of local privacy and technology experts across North America, Asia, and Europe.

OneTrust is backed by the founders of Manhattan Associates (NASDAQ: MANH) and AirWatch (\$1.54B acq by VMWare).



The advertisement features a green header with the OneTrust logo and the text "Privacy Management Software". Below this, a dark grey banner reads "The #1 Cross-Jurisdictional Privacy Management Software". In the center is a laptop displaying a dashboard with four circular progress indicators: "GDPR Privacy Impact Assessments (PIA / DPIA)" at 72%, "GDPR Privacy Data Mapping Automation" at 21%, "GDPR Privacy Vendor Risk Management" at 21%, and "GDPR Privacy Incident Management" at 72%. To the right of the laptop is a world map with a red line connecting North America and Europe. Below the laptop, the text "OneTrust.com" is displayed in green. On either side of the laptop are two columns of bulleted features.

OneTrust
Privacy Management Software

The #1 Cross-Jurisdictional Privacy Management Software

- GDPR Centralized Records
- Privacy Impact Assessments (PIA / DPIA)
- Data Mapping Automation
- Intelligent Identity Scanning

- EU Cookie Compliance
- Subject Rights Requests
- Consent Management
- Vendor Risk Management
- Incident Management

OneTrust.com