WHAT DOES IT MEAN TO ME?

# GDPR DATA PROTECTION IMPACT ASSESSMENTS

ISACA®

**ABSTRACT**

In 2016, the European Union General Data Protection Regulation (GDPR) (effective on 25 May 2018) was adopted to replace the Directive 95/46/EC to implement a legally binding regulation that will be considered the EU data protection law. EU data protection law provides data subjects with a wide range of rights that can be enforced against enterprises that process personal data. These rights will limit the ability of enterprises to lawfully process the personal data of data subjects in many of the ways that were regularly employed in the past. These new rights can significantly impact an enterprise's business model. The shift to a protection model that is focused on individual privacy represents a major transformation in the requirements for protecting the personal data of individuals throughout Europe.

Given the significant financial penalties for noncompliance and evidently more proactive compliance efforts planned by the EU data protection supervisor, the GDPR truly compels action from not only all enterprises that are doing business across Europe (including the United Kingdom post-Brexit, the EU and European Economic Area countries), but also all enterprises with offices in Europe, workers in Europe (even if they are not located there permanently), and clients, customers, patients and any type of consumer in Europe. A significant requirement of GDPR is for enterprises to conduct data protection impact assessments (DPIAs) to identify and reduce the data protection risk within projects and systems, and reduce the likelihood of privacy harms to data subjects.

# CONTENTS

# GDPR Data Protection Impact Assessments

## How to Perform GDPR-required DPIAs Using ISACA Privacy Principles

## Introduction and Objectives

News reports about privacy breaches and associated privacy fines and penalties are continuing to increase.[1,2] More data are being created[3] that are associated with specific individuals, which increases privacy risk. As a result, more legal requirements are being imposed to protect personal data. One of the most talked about looming set of legal requirements goes into effect on 25 May 2018—the EU General Data Protection Regulation (GDPR).[4,5]

The EU GDPR replaces the Data Protection Directive 95/46/EC that has been in force since 1995.[6] The GDPR is designed to harmonize personal data protection laws that provide privacy protections across the European Union and reshape the way enterprises approach data privacy. Every enterprise that has the personal data of an individual who is located in the EU needs to be in compliance with the GDPR by 25 May 2018. If an enterprise is not in compliance when a GDPR supervisory authority conducts an audit, the enterprise faces large penalties, up to €20 million, or up to four percent of the enterprise's total worldwide annual revenue for the preceding financial year, whichever is greater.[7]

This paper provides readers with information about the EU GDPR, the benefits of using the ISACA privacy principles to perform GDPR-required data protection impact assessments (DPIAs), which are a specific type of privacy impact assessment (PIA), and how to accomplish GDPR DPIAs using the privacy principles. Readers are given a link to an accompanying tool that provides even more help with performing GDPR DPIAs. The concepts in this paper can also be used for performing traditional PIAs, which, historically, have not covered all the requirements of GDPR DPIAs.

1 For an example of the increase in the hospitality space, see Tran, Canh; "The Rise in Hotel & Restaurant Data Breaches," Rippleshot, 17 February 2016, *http://info.rippleshot.com/blog/the-rise-in-hotel-restaurant-data-breaches*

2 For an example in the United Kingdom, see Information Commissioner's Office, "Data security incident trends," ico., *https://ico.org.uk/action-weve-taken/data-security-incident-trends/*

3 For example, in 300 seconds, 7,065,662 GB of data were created on the Internet. See Desreumaux, Geoff; "The Impressive Real-Time Growth of the Internet," WeRSM, 4 September 2016, *http://wersm.com/the-impressive-real-time-growth-of-the-internet-2*

4 European Data Protection Supervisor, "The History of the General Data Protection Regulation," *https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en*

5 Official Journal of the European Union, "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016," *http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&qid=1499881815698&from=EN*

6 "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," *Official Journal*, L 281, 23/11/1995 P. 0031 – 0050, 31995L0046, *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML*

7 General Data Protection Regulation (GDPR), "Art. 83 GDPR General conditions for imposing administrative fines," *https://gdpr-info.eu/art-83-gdpr/*

## GDPR Requirements and Impact

The GDPR contains more requirements than the EU Data Protection Directive 95/46/EC and includes the following significant general changes:[8]

- Territorial scope is increased with extraterritorial applicability.
- Penalties can be applied to data controllers and data processors.[9]
- Consent conditions are strengthened and requirements are more stringent.
- Breach notification is to data subjects and to supervisory authorities, within 72 hours of breach identification.
- Right to access applies to associated personal data, actions and reports.
- Right to be forgotten includes erasing personal data and halting personal data processing.
- Data portability allows data subjects to be provided with their personal data upon request and in a format that facilitates transmission to another data controller.
- Privacy by design includes data protection controls and safeguards throughout the full design life cycle of systems, applications and other processes.
- Formally assigned data protection officers perform internal recordkeeping requirements.
- Data protection impact assessments (a privacy impact assessment that is specific to GDPR requirements) must be performed by the data protection officer.

The GDPR effect is not isolated to the European Union. GDPR applicability makes a global impact. When GDPR goes into effect, all enterprises that have any type of personal information within EU countries need to comply with the hundreds of associated requirements within the 99 articles.[10,11] The GDPR applies to enterprises that have:

- Personnel in business locations of any type (e.g., office, manufacturing plant or distribution center) in the European Union
- Employees, contractors, consumers, customers, patients or other people who are citizens of, located within or currently traveling through the European Union
- Processing that includes some type of monitoring of individuals within, or who are citizens of, the European Union
- Goods and/or services that are available to individuals located within the European Union

Hundreds of millions of enterprises worldwide need to be in compliance with the GDPR by the 2018 deadline or face severe penalties. If enterprises have not begun work to meet all compliance requirements, they must start now.

**Figure 1** shows the decision-making process for determining if an enterprise is legally bound to the requirements of the GDPR.

GDPR is applicable to most large enterprises and to a significant portion of small-to-midsized enterprises.

8 GDPR Portal, "GDPR Key Changes," *http://www.eugdpr.org/key-changes.html*

9 Throughout this paper, the terms data controller and data processor refer to the names of the roles the GDPR uses for the people or enterprises that control or process personal data.

10 See the list of current EU countries at European Union, "EU member countries in brief," 13 September 2017, *https://europa.eu/european-union/about-eu/countries/member-countries_en*

11 *Op cit* Official Journal of the European Union

Therefore, it is imperative that practitioners understand the GDPR requirements, how to assess whether the enterprise is in compliance with them and implement the specific GDPR requirements that are applicable to the enterprise, according to the decision tree in **figure 1**. Regardless of their role within the enterprise, practitioners who are charged with establishing the value from, and trust in, information and information systems are impacted by GDPR and potentially by the DPIA process. Specifically, the following roles are impacted:

- Audit, assessment and assurance practitioners
- Information security and cyber security practitioners
- Compliance practitioners
- Governance professionals
- Privacy professionals and legal counsel
- Risk practitioners and risk managers

The following sections describe the EU GDPR impacts that are associated with each role.

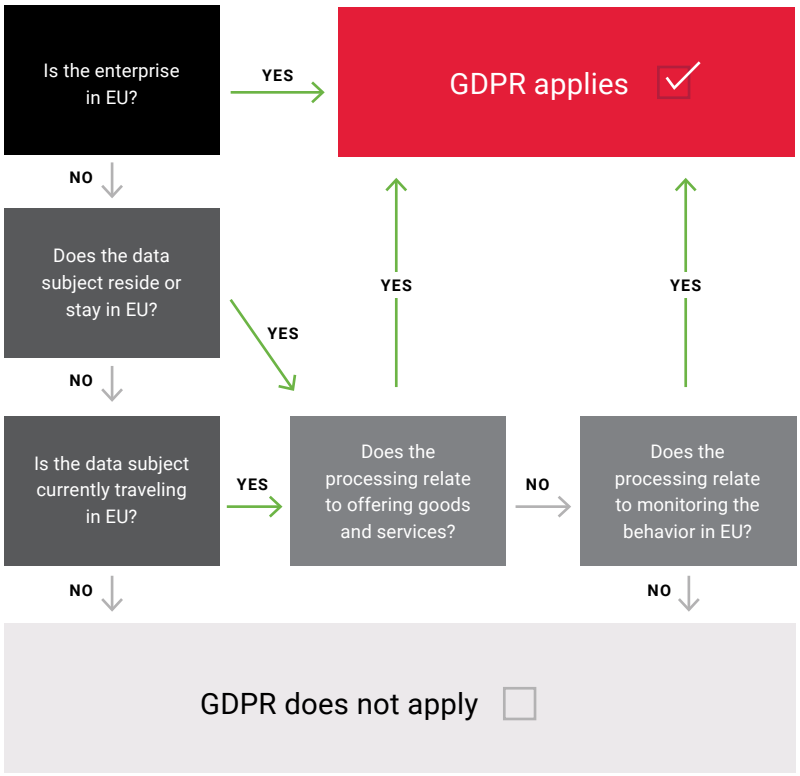


**FIGURE 1:** Determining if GDPR Applies to an Enterprise

Source: Varankevich, Siarhei; "Territorial scope of the GDPR (Flowchart)," LinkedIn, 17 February 2017, *www.linkedin.com/pulse/territorial-scope-gdpr-flowchart-siarhei-varankevich*, adapted per creative commons license at *https://creativecommons.org/licenses/by-sa/4.0/*

## Audit, Assessment and Assurance

Auditors are impacted by the GDPR in the same way they are impacted by any governing regulation to which the enterprise is subject.

Auditors are required to:

- Evaluate the enterprise's overall posture from a privacy perspective
- Ensure that DPIAs are performed as required by the regulation and that other specific regulatory mandates are met
- Ensure that privacy is accounted for in audit planning
- Evaluate the controls that support privacy initiatives and the completion of all required artifacts, including DPIAs.

## Information Security and Cyber Security

Information security and cyber security practitioners are, likewise, impacted by the GDPR and the DPIA process. From a control selection and operations standpoint, the controls that support privacy are likely to overlap directly or indirectly with those that support confidentiality of data in other contexts. Moreover, aspects of testing and monitoring—such as vulnerability assessment, log management, penetration testing and other detective controls—are

applicable to security and privacy efforts in tandem. Beyond this, the DPIA itself can be used to inform security efforts; the data gathered during the DPIA process can be a source for security and information protection efforts.

### Compliance

Compliance practitioners have responsibility for ensuring ongoing adherence to all governing regulation, including legislative requirements from multiple jurisdictions. Therefore, the DPIA and the compliance aspects of GDPR are directly applicable to the compliance practitioner for:

- Monitoring and tracking
- Harmonizing specific GDPR requirements with other regulations and regulatory frameworks
- Integrating GDPR compliance efforts into the overall enterprise compliance program

### Governance

As evidenced by ISACA's recent privacy guidance,[12,13] privacy management can be a critical and foundational element of robust governance—an enterprise goal to which resources are applied. Likewise, privacy considerations directly map to enablers that help the enterprise meet critical stakeholder goals. Privacy represents a potential risk area that should be a part of risk management and risk assessment efforts; therefore, privacy should be included in governance planning and risk management activities.

### Privacy

The GDPR is germane to privacy; therefore, privacy practitioners represent the role with the highest impact from this regulation.

### Risk

Privacy represents an area of regulatory risk and potentially reputational risk for many enterprises. Therefore, risk management professionals need to account for the risk dynamics of privacy, including, and driven directly from, the results of the DPIA. Assessment efforts should account for privacy to the same degree that they account for other areas of potential risk.

## Using the ISACA Privacy Principles to Perform GDPR DPIAs

The GDPR requires each data controller and data processor to perform DPIAs.[14] These go beyond traditional PIAs, which focus on risk that is primarily to the enterprise itself. The DPIA process is designed to:

- Describe the processing
- Assess the necessity and proportionality of processing
- Determine compliance with the GDPR requirements
- Help manage the risk to the rights and freedoms of natural persons that results from processing personal data, and determine appropriate measures to address this risk

DPIAs also support accountability by helping data controllers and data processors not only to comply with all the requirements of the GDPR, but also to demonstrate due diligence that the enterprise is taking appropriate actions to ensure full compliance on an ongoing basis.

12 ISACA, *ISACA Privacy Principles and Program Management Guide*, USA, 2016, *www.isaca.org/Knowledge-Center/Research/Pages/Privacy.aspx*

13 ISACA, *Implementing a Privacy Protection Program: Using COBIT® 5 Enablers With the ISACA Privacy Principles*, USA, 2017, *www.isaca.org/Knowledge-Center/Research/Pages/Privacy.aspx*

14 General Data Protection Regulation (GDPR), "Art. 35 GDPR Data protection impact assessment," *https://gdpr-info.eu/art-35-gdpr/*

Article 35 of the GDPR is specific about the topics that are required to be considered within an acceptable DPIA. These topics include:

- Applicability—when and for what types of processing DPIA must be performed (article items 1, 3, 10, 11)[15]
- Roles and responsibilities of the data protection officer and the applicable supervisory authority (article items 2, 4, 5, 6)[16]
- Required elements of, and considerations for, a DPIA (article items 7, 8, 9)[17]

Following is the excerpt of items 7, 8 and 9 of Article 35 of the GDPR detailing the necessary components of the DPIA.[18]

*7. 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;*

*(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*

*(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and*

*(d) 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 this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.*

*8. Compliance with approved codes of conduct referred to in **Article 40** by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.*

*9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.*

15 *Ibid.*
16 *Ibid.*
17 *Ibid.*
18 *Ibid.*

## Relationship of ISACA Privacy Principles to GDPR Requirements

In addition to the GDPR, most enterprises must also ensure compliance with multiple other legal requirements for personal data by performing PIAs. Including the other personal data protection requirements in the DPIA process for the GDPR is the most efficient and beneficial approach for an enterprise, regarding resources and time.

Enterprises can use the ISACA privacy principles as the framework for their DPIA by following these steps:

1. Group the GDPR and other requirements within each of the 14 privacy principles.
2. Address the GDPR requirements through questions that apply to the DPIA.
3. Adjust the questions so that they apply to the similar requirements from the other data protection legal obligations.
4. Address the other requirements through the adjusted questions.

This consolidated approach accomplishes the GDPR DPIA and the required PIAs for the other privacy principles and standards, eliminating the need to perform separate PIAs. Often, compliance with the legal requirements of the other privacy principles and standards have already been mapped to existing standards, such as the Organisation for Economic Co-operation and Development (OECD) privacy guidelines,[19] the Asia-Pacific Economic Cooperation (APEC) privacy framework,[20] the ISO/IEC 29100 Information technology — Security techniques — Privacy framework,[21] and the US National Institute of Standards and Technology (NIST) SP 800-53A Assessing Security and Privacy Controls in Federal Information Systems and Enterprises.[22]

**Figure 2** shows how each of the privacy principles maps to the GDPR and some of the similar requirements from the other privacy principles and standards that an enterprise can address while performing a GDPR DPIA. Enterprises can create a mapping that is similar to **figure 2**, so that they have documentation showing how the GDPR topics and privacy principles also cover a wide range of requirements from other standards, guidelines and frameworks.

**Figure 3** shows how the fourteen ISACA privacy principles map to the specific GDPR Articles with requirements. Enterprises can use this figure to assess the personal data risk and harms when performing the DPIA.

All of the requirements that need to be assessed in a GDPR DPIA to determine the risk levels and progress with compliance can be mapped to the 14 ISACA privacy principles.

## Questions to Address During DPIA

This section provides examples of the types of questions that data controllers and data processors should ask for each privacy principle during the DPIA. Three examples are provided for each privacy principle, but enterprises that perform DPIAs need to ask the sufficient number of questions to accurately determine the compliance and risk level for their business environments.

19 OECD, "2013 OECD Privacy Guidelines," *https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm*

20 APEC, "APEC Privacy Framework," *http://publications.apec.org/publication-detail.php?pub_id=390*

21 International Organization for Standardization, "ISO/IEC 29100:2011 Information technology -- Security techniques -- Privacy framework," *https://www.iso.org/standard/45123.html*

22 NIST, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations," NIST Special Publication 800-53A, Revision 4, December 2014, *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf*

| ISACA PRIVACY PRINCIPLES | GDPR | ISO 29100:2011 | APEC | GAPP |
|---|---|---|---|---|
| **1. Choice and Consent** | Notice & Consent | Consent and choice | Choice | Choice and consent |
| **2. Legitimate Purpose Specification and Use Limitation** | Legitimate Purpose and Automated Decision-Making | Purpose legitimacy and specification; and Use, retention and disclosure limitation | Use of personal Information | Use, retention and disposal |
| **3. Personal Information and Sensitive Information Life Cycle** | Privacy by Design, DPIAs, Data Subject Participation & Safe-guards | Collection limitation; and Data minimization | Collection limitations | Collection |
| **4. Accuracy and Quality** | Data Rectification & Data Quality | Accuracy and quality | Integrity of personal information | Quality |
| **5. Openness, Transparency and Notice** | Transparency & Data Subject Rights | Openness, transparency and notice | N/A | N/A |
| **6. Individual Participation** | Data Subject Access | Individual participation and access | Access and correction | Access |
| **7. Accountability** | Data Processing, Data Protection Officers & Controllers | Accountability | Accountability | Management |
| **8. Security Safeguards** | Security Safeguards Throughout Data Lifecycle | Information security | Security safeguards | Security for privacy |
| **9. Monitoring, Measuring and Reporting** | Processing, Right to be Forgotten & Data Portability Records/ Reports | Privacy compliance | N/A | Monitoring and enforcement |
| **10. Preventing Harm** | Lawfulness, Data Subject Access, Portability & DPIAs | N/A | Preventing harm | N/A |
| **11. Third-party/Vendor Management** | Processors Management | N/A | N/A | Disclosure to third parties |
| **12. Breach Management** | Breach Management & Notifications | N/A | N/A | N/A |
| **13. Security and Privacy by Design** | Controller Respon-sibilities, Automated Decision-Making & Data Protection by Default | N/A | N/A | N/A |
| **14. Free Flow of Information and Legitimate Restriction** | Data Subject Rights, Lawfulness, Data Transfers, Binding Corporate Rules | N/A | N/A | N/a |

**FIGURE 2:** ISACA Privacy Principles Mapped to Major Privacy Principles and Standards

| ISACA PRIVACY PRINCIPLES | RELATED GDPR ARTICLES |
|---|---|
| **1. Choice and Consent** | Article 6: Lawfulness of processing<br>Article 7: Conditions for consent<br>Article 8: Conditions applicable to child's consent in relation to information society services |
| **2. Legitimate Purpose Specification and Use Limitation** | Article 5: Principles relating to processing of personal data<br>Article 6: Lawfulness of processing<br>Article 10: Processing of personal data relating to criminal convictions and offences<br>Article 22: Automated individual decision-making, including profiling<br>Article 39: Tasks of the data protection officer |
| **3. Personal Information and Sensitive Information Life Cycle** | Article 5: Principles relating to processing of personal data<br>Article 6: Lawfulness of processing<br>Article 9: Processing of special categories of personal data<br>Article 21: Right to object<br>Article 25: Data protection by design and by default<br>Article 35: Data protection impact assessment<br>Article 89: Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes |
| **4. Accuracy and Quality** | Article 5: Principles relating to processing of personal data<br>Article 16: Right to rectification |
| **5. Openness, Transparency and Notice** | Article 5: Principles relating to processing of personal data<br>Article 12: Transparent information, communication and modalities for the exercise of the rights of the data subject<br>Article 13: Information to be provided where personal data are collected from the data subject<br>Article 14: Information to be provided where personal data have not been obtained from the data subject<br>Article 15: Right of access by the data subject<br>Article 21: Right to object |
| **6. Individual Participation** | Article 7: Conditions for consent<br>Article 12: Transparent information, communication and modalities for the exercise of the rights of the data subject<br>Article 14: Information to be provided where personal data have not been obtained from the data subject<br>Article 15: Right of access by the data subject<br>Article 16: Right to rectification<br>Article 17: Right to erasure ('right to be forgotten')<br>Article 18: Right to restriction of processing<br>Article 20: Right to data portability<br>Article 21: Right to object<br>Article 22: Automated individual decision-making, including profiling<br>Article 26: Joint controllers<br>Article 38: Position of the data protection officer |
| **7. Accountability** | Article 5: Principles relating to processing of personal data<br>Article 6: Lawfulness of processing<br>Article 14: Information to be provided where personal data have not been obtained from the data subject<br>Article 24: Responsibility of the controller<br>Article 27: Representatives of controllers or processors not established in the Union<br>Article 32: Security of processing<br>Article 36: Prior consultation<br>Article 37: Designation of the data protection officer<br>Article 38: Position of the data protection officer<br>Article 39: Tasks of the data protection officer |

**FIGURE 3:** ISACA Privacy Principles Mapped to GDPR Requirements

| ISACA PRIVACY PRINCIPLES | RELATED GDPR ARTICLES |
|---|---|
| **8. Security Safeguards** | Article 5: Principles relating to processing of personal data<br>Article 6: Lawfulness of processing<br>Article 24: Responsibility of the controller<br>Article 32: Security of processing<br>Article 46: Transfers subject to appropriate safeguards |
| **9. Monitoring, Measuring and Reporting** | Article 17: Right to erasure ('right to be forgotten')<br>Article 19: Notification obligation regarding rectification or erasure of personal data or restriction of processing<br>Article 20: Right to data portability<br>Article 30: Records of processing activities<br>Article 33: Notification of a personal data breach to the supervisory authority<br>Article 34: Communication of a personal data breach to the data subject<br>Article 35: Data protection impact assessment<br>Article 37: Designation of the data protection officer<br>Article 39: Tasks of the data protection officer<br>Article 47: Binding corporate rules |
| **10. Preventing Harm** | Article 6: Lawfulness of processing<br>Article 15: Right of access by the data subject<br>Article 20: Right to data portability<br>Article 22: Automated individual decision-making, including profiling<br>Article 35: Data protection impact assessment<br>Article 89: Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes<br>Article 91: Existing data protection rules of churches and religious associations |
| **11. Third-party/Vendor Management** | Article 28: Processor<br>Article 29: Processing under the authority of the controller or processor<br>Article 32: Security of processing |
| **12. Breach Management** | Article 33: Notification of a personal data breach to the supervisory authority<br>Article 34: Communication of a personal data breach to the data subject |
| **13. Security and Privacy by Design** | Article 22: Automated individual decision-making, including profiling<br>Article 24: Responsibility of the controller<br>Article 25: Data protection by design and by default |
| **14. Free Flow of Information and Legitimate Restriction** | Article 6: Lawfulness of processing<br>Article 21: Right to object<br>Article 44: General principle for transfers<br>Article 45: Transfers on the basis of an adequacy decision<br>Article 46: Transfers subject to appropriate safeguards<br>Article 47: Binding corporate rules<br>Article 48: Transfers or disclosures not authorized by Union law<br>Article 49: Derogations for specific situations |

**FIGURE 3:** ISACA Privacy Principles Mapped to GDPR Requirements (continued)

Within the context of this section, the following terms are defined as follows:

- **Information:** Personal information and sensitive information, collectively
- **Processing:** The collection, derivation, use, disclosure, analysis, processing, storage, transfer, retention, disposal and any other type of access to personal information and sensitive information
- **Business environment:** Includes size (number of employees, amount of revenues, etc.); locations of the business and its contracted vendors; industries; residencies and business locations of employees, clients, consumers, patients, etc.; and existing legal requirements.

**NOTE:**
More detailed descriptions of the privacy principles are in the *ISACA Privacy Principles and Program Management Guide*.[23]

### 1. CHOICE AND CONSENT PRINCIPLE

When data controllers/data processors collect personal information from data subjects, the data controllers/data processors should describe choices that are available to the data subjects and obtain appropriate consents, in ways appropriate to the context of each situation.

To determine privacy risk, potential data subject privacy harms and GDPR compliance gaps related to this topic within a DPIA, answer the following questions and verify the associated GDPR requirements cited for each:

- Do you have documented and enforced privacy policies and supporting procedures to provide choices where appropriate? (Article 6(1))
- Are obtained consents appropriately documented and maintained? (Article 7(1), Article 7(2))
- If your enterprise collects information from children younger than 16 years old, have you created documented policies and implemented processes to collect parental consent as required by the GDPR? (Article 8(1))

### 2. LEGITIMATE PURPOSE SPECIFICATION AND USE LIMITATION PRINCIPLE

This generally requires that data controllers/data processors clearly describe to data subjects and data protection authorities, as appropriate, the purposes for collecting information and then limit information processing to only those purposes.

To determine privacy risk, potential data subject privacy harms and GDPR compliance gaps related to this topic within a DPIA, answer the following questions and verify the associated GDPR requirements cited for each:

- Do you have documented and enforced privacy policies and supporting procedures to obtain consent for, collect and process only the personal data that is adequate, relevant and limited to the purposes for which they were collected and will be processed? (Article 5(1), Article 6(1))
- Do you have mechanisms and controls in place to ensure that any intended further processing is reviewed and the appropriate action is taken prior to such use (e.g., obtaining data subject consent and ensuring legal compliance)? (Article 6(4)(a))
- Have you determined and documented the situations in which the right to object does not apply, and have you implemented appropriate supporting procedures to apply in these situations? (Article 22(2))

23 *Op cit* ISACA, *ISACA Privacy Principles and Program Management Guide*

### 3. PERSONAL INFORMATION AND SENSITIVE INFORMATION LIFE CYCLE PRINCIPLE

Data controllers/data processors are generally required to limit the collection and all uses of information to the specified documented purposes, and then ensure that information processing aligns with those specified purposes throughout the entire processing life cycle, including data retention and disposal. If additional processing is pursued at any point throughout the life cycle, then consents and/or data protection authority approval, as appropriate to the situation, must be obtained first.

To determine privacy risk, potential data subject privacy harms and GDPR compliance gaps related to this topic within a DPIA, answer the following questions and verify the associated GDPR requirements cited for each:

- Do you have documented and enforced privacy policies and supporting procedures to keep personal data for no longer than necessary to support the purposes for which they were collected, while in support of legal and any applicable public interest, scientific and historic research purposes? (Article 5(1))
- Have you established methods and technologies that allow data subjects to request to be removed from the data controller/data processor processes that are using their personal data for direct-marketing purposes? (Article 21(3))
- Do you have documented and enforced privacy policies and supporting procedures that require the implementation of appropriate technical and data controller/data processor measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed? (Article 25(2))

### 4. ACCURACY AND QUALITY PRINCIPLE

Data controllers/data processors are generally required to ensure that information is as accurate, complete and up to date as necessary to limit the risk that inaccurate information is used for decision-making.

To determine privacy risk, potential data subject privacy harms and GDPR compliance gaps related to this topic within a DPIA, answer the following questions and verify the associated GDPR requirements cited for each:

- Do you have a mechanism in place to correct personal data when necessary, in all locations of the data? (Article 5(1))
- Do you have documentation that logs or lists all corrections to personal data, including date, time, who made the change, etc.? (Article 5(2))
- Do you have a process to allow data subjects a method for requesting corrections to errors within their personal data? (Article 16)

### 5. OPENNESS, TRANSPARENCY AND NOTICE PRINCIPLE

Data controllers/data processors are generally required to provide clear, accessible and accurate details about their privacy management program, how information is processed and the timing for providing this information.

To determine privacy risk, potential data subject privacy harms and GDPR compliance gaps related to this topic within a DPIA, answer the following questions and verify the associated GDPR requirements cited for each:

- Do you have documented and enforced privacy notices, policies and supporting procedures and processes to communicate data subject rights and information describing processing in a clear, easy-to-understand and age-appropriate manner? (Article 12(1))
- Do you have documented and enforced privacy policies and supporting procedures and processes to provide data subjects with information describing any other purposes for which already collected personal information will be used, prior to further processing? (Article 13(3), Article 14(4))
- Do you have documented and enforced privacy policies and supporting procedures and processes to inform data subjects of the safeguards used when personal data are transferred to a third country or to an international data controller/data processor? (Article 15(2))
- At the time when personal data are obtained, do you provide the data subject with further information relating to the existence of the right to data portability? (Article 13(2))
- Do you provide the data subject with information about the existence of automated decision making, including profiling, meaningful information about the logic involved, and the significance and intended goals of profiling for the data subject? (Article 14(2))

### 6. INDIVIDUAL PARTICIPATION PRINCIPLE

Data controllers/data processors are generally required to provide data subjects with rights for accessing, porting elsewhere, reviewing, confirming, correcting, restricting use of and deleting their associated information, and withdrawing existing consents that they provided. Easy-to-use methods are required to be provided to accomplish these rights.

To determine privacy risk, potential data subject privacy harms and GDPR compliance gaps related to this topic within a DPIA, answer the following questions and verify the associated GDPR requirements cited for each:

- Do you have documented and enforced privacy policies, supporting procedures and easy-to-use processes to allow data subjects to withdraw consent to use their associated personal data at any time, including personal data used in partnership with other data controllers, as long as the withdrawal does not result in legal violations about which you have informed the data subjects? (Article 7(3), Article 26(3))

- Do your procedures and methods, in partnership with any other joint data controllers, allow a verified data subject to exercise his or her rights to request access to, information about, corrections to, deletion/destruction of, or restrictions on his or her associated personal data in compliance with the timing, costs and format of information delivery requirements under the GDPR? (Article 12(2), Article 12(3), Article 12(4), Article 12(5), Article 12(6), Article 14(3), Article 16, Article 26(3))
- Do you have a mechanism implemented to allow a verified data subject the ability to obtain confirmation about whether or not personal data concerning him or her are being processed, and, if so, to give the data subject access to the personal data and provide information concerning the purposes, categories, recipients, retention periods, rights for deletion and making complaints, ability to restrict personal data processing where feasible, legal notices when restrictions are lifted and data source details when possible? (Article 15(1), Article 18)

**7. ACCOUNTABILITY PRINCIPLE**

Data controllers/data processors are generally required to take actions to demonstrate accountability throughout their workforce for appropriate governance and risk management of the information for which they have responsibility, and to ensure associated activities are performed in compliance with all associated legal requirements.

To determine privacy risk, potential data subject privacy harms and GDPR compliance gaps related to this topic within a DPIA, answer the following questions and verify the associated GDPR requirements cited for each:

- Do you have documented and enforced privacy policies and supporting procedures that establish the requirements for the data protection officer's responsibilities and the actions for which the data protection officer is responsible, ensuring that the persons fulfilling this role are appropriately qualified and knowledgeable? (Article 37(1), Article 37(2); Article 37(3); Article 37(4), Article 37(5), Article 37(6))
- Do you have documented and enforced privacy policies and supporting procedures to ensure accountability for designated roles within your enterprise to communicate appropriately with data subjects when their associated information is not obtained directly from them? (Article 14(1))
- Do you have processes in place to ensure accountability for a specific role within the enterprise to consult with the appropriate supervisory authority prior to processing, if a data protection impact assessment indicates that the processing results in high risk in the absence of measures taken to mitigate the risk? (Article 36(1), Article 36(3))

**8. SECURITY SAFEGUARDS PRINCIPLE**

Data controllers/data processors are generally required to ensure that appropriate security safeguards are in place for all information throughout the enterprise and the entire information life cycle, in any location where it is processed.

To determine privacy risk, potential data subject privacy harms and GDPR compliance gaps related to this topic within a DPIA, answer the following questions and verify the associated GDPR requirements cited for each:

- Do you have documented and enforced security policies and supporting procedures to ensure that information has appropriate safeguards to secure the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage? (Article 5(1), Article 24(2))
- Have you implemented methods and technologies to assess the likelihood of privacy harms to data subjects if unauthorized sharing, unauthorized use, unauthorized or accidental destruction of, loss of, changes to and other access to personal data occurs, and then to implement appropriate technical and data controller/data processor measures to ensure a level of security for the personal data that is appropriate to the personal harm risk? (Article 32(1), Article 32(2))
- Do you follow documented procedures and use technologies implemented to ensure safeguards for information transferred to a third country[24] or international data controller/data processor? (Article 46(1))

**9. MONITORING, MEASURING AND REPORTING PRINCIPLE**

Data controllers/data processors are generally required to implement appropriate and consistent monitoring, measuring and reporting capabilities to determine the effectiveness of the privacy management program and tools.

To determine privacy risk, potential data subject privacy harms and GDPR compliance gaps related to this topic within a DPIA, answer the following questions and verify the associated GDPR requirements cited for each:

- Do you have documented policies and supporting procedures detailing the reports and tasks for which the data protection officer is responsible in order to validate that the data controller/data processor is providing sufficient regular privacy and security training and ongoing awareness communication to staff, and to record the attendance details and descriptions of the topics covered? (Article 39(1))
- Do you have processes and any necessary associated technologies implemented for creating reports to provide to data subjects that provide details about their associated personal data erasures or incorrect personal data? (Article 19)
- Do you follow required processes to create communications to appropriate supervisory authorities that include the contact information for the data protection officer and personal data breach reports? (Article 37(7), Article 33(5))

**10. PREVENTING HARM PRINCIPLE**

Data controllers/data processors are generally required to have processes and implement tools to identify and document the potential privacy harms to data subjects if the information for which the data controller/data processor is responsible is misused or breached.

To determine privacy risk, potential data subject privacy harms and GDPR compliance gaps related to this topic within a DPIA, answer the following questions and verify the associated GDPR requirements cited for each:

- Do you have documented data-subject harm prevention policies and supporting procedures that specify how to determine that personal data processing is lawful under at least one of the following conditions:
  a) the associated data subject provides explicit consent;
  b) the processing is required to fulfill a contract with the data subject;
  c) the processing reflects a legal obligation;
  d) the processing protects vital interests of natural persons;

24 A third country is a country to which personal data are sent from a second country, which is the original recipient of the transferred data.

e) the processing is required for tasks necessary to the public interest; or

f) the processing is required for legitimate interests of the data controller/data processor or its third parties? (Article 6(1))

- Do you have procedures that are consistently followed to ensure that decisions relating to data subjects must not be made based on special categories of personal data unless specific safeguards have been implemented? (Article 22(4))
- Do you have documented data-subject harm prevention policies, supporting procedures and implemented processes, and tools to ensure that data subjects who exercise their rights for changing how their personal data are used and for requesting copies of personal data and other types of rights under GDPR do not adversely affect the rights and freedoms of others? (Article 15(4), Article 20(4))

**11. THIRD-PARTY/VENDOR MANAGEMENT PRINCIPLE**

Data controllers/data processors are generally required to establish and implement appropriate policies, processes and tools to provide for ongoing oversight of the third parties to which they entrust any type of access to information for which the data controller/data processor is responsible.

To determine privacy risk, potential data subject privacy harms and GDPR compliance gaps related to this topic within a DPIA, answer the following questions and verify the associated GDPR requirements cited for each:

- Do you have documented third-party/vendor management policies and supporting procedures to ensure that your enterprise does not use third-party/vendor processors unless they provide sufficient guarantees and verified proof that they have implemented appropriate technical and data controller/data processor (physical and administrative) measures and controls to support data subject rights, and they contractually agree to notify your enterprise whenever any changes occur involving adding or removing other involved processors? (Article 28(1), Article 28(2))
- Do you have documented procedures that detail the actions that third-party/vendor processors must take, and the proof that they must collect, if they engage other processors to carry out specific processing activities that are part of the activities your enterprise had contracted the processor to perform, and to ensure such subcontracting includes the same requirements that the processor agreed to within the contract they have with your enterprise? (Article 28(4), Article 28(5))

- Do you have documented third-party/vendor management policies and supporting procedures that detail the steps that your enterprise must take to ensure that natural persons who are acting under the authorities of your enterprise and your third-party/vendor and who have access to personal data follow all personal data policies and procedures, instructions provided by your enterprise or the third-party/vendor for which the natural persons work and associated rules and requirements established by Union or member state law? (Article 32(4), Article 29)

**12. BREACH MANAGEMENT PRINCIPLE**

Data controllers/data processors are generally required to establish policies, procedures and methods to prevent, identify quickly, respond to and effectively mitigate privacy breaches.

To determine privacy risk, potential data subject privacy harms and GDPR compliance gaps related to this topic within a DPIA, answer the following questions and verify the associated GDPR requirements cited for each:

- Do you have documented personal data breach policies and supporting procedures that include requirements for notifying appropriate supervisory authorities of the breach in a timely manner and with reasons for any delays? (Article 33(1))
- Do you have documented procedures and supporting tools for notifying data subjects, without delay and no later than 72 hours following the discovery of a breach, if it is determined, following documented procedures for performing harm/risk analysis, that the personal data breach will result in privacy harm to the associated data subjects? (Article 33(1), Article 33(2))
- Do you have processes and mechanisms in place to document and create a report for each personal data breach, including the facts relating to the breach, the possible effects of the breach to the associated data subjects and the remedial action that your enterprise takes in response? (Article 33(5))

**13. SECURITY AND PRIVACY BY DESIGN PRINCIPLE**

Data controllers/data processors are generally required to document the enterprise privacy philosophy and its supporting policies and procedures by which the enterprise performs business activities with built-in security and privacy protections.

To determine privacy risk, potential data subject privacy harms and GDPR compliance gaps related to this topic within a DPIA, answer the following questions and verify the associated GDPR requirements cited for each:

- Do you have documented procedures and supporting implemented technologies to build security and privacy protections into the full life cycle of automated decision-making processes involving personal data? (Article 22(3))
- Do you have mechanisms implemented to allow the data subjects to include their points of view in their associated records regarding decisions about their associated personal data and to allow the data subjects to contest the decisions? (Article 22(3))
- Do you have documented and enforced policies and supporting procedures to assess the risk associated with the nature, scope, context and purposes of processing personal data and the associated likelihood and severity of harms for data subjects? (Article 24(1))

#### 14. FREE FLOW OF INFORMATION AND LEGITIMATE RESTRICTION PRINCIPLE

Data controllers/data processors are generally required to document the enterprise privacy philosophy and its supporting policies and procedures by which the enterprise safeguards personal data sent across country borders in support of business activities.

To determine privacy risk, potential data subject privacy harms and GDPR compliance gaps related to this topic within a DPIA, answer the following questions and verify the associated GDPR requirements cited for each:

- Do you have documented and enforced policies and supporting procedures to contact the appropriate supervisory authority, using an associated established consistent mechanism, to approve required corporate rules to ensure that they are legally binding, include all necessary and appropriate data protections, are consistently enforced, and provide all legally required data subject rights? (Article 47(1))
- Do you have documented procedures to follow for transfers of personal data to a third country or to an international data controller/data processor that state that this transfer can occur only after certain conditions (adequacy, international agreement, verified existence of appropriate safeguards, enforceable data subject rights and available effective legal remedies) have been validated? (Article 44, Article 45, Article 46(1))
- Do you have enforced data security policies and supporting procedures and mechanisms implemented for personal data transfer safeguards that are applicable for each situation and are legally documented with public authorities, binding corporate rules, standard data protection clauses from the commission or applicable supervisory authority, approved codes of conduct or approved certification mechanisms? (Article 46(2))

### A DPIA Tool

ISACA provides the GDPR DPIA Tool at www.isaca.org/GDPR-DPIA to guide enterprises in performing a generic DPIA for all types of enterprises. This tool provides more questions for each of the principles and a section that enterprises can use to document the remaining necessary requirements, including:

- Scope of the processing
- Applicability—when and for what types of processing DPIA must be performed
- Roles and responsibilities of the data protection officer and the applicable supervisory authority

## Ongoing Privacy Risk Management

Enterprises are not done complying with the GDPR after they perform the DPIA—stopping compliance efforts is not in compliance with the GDPR.

Following the conclusion of a DPIA, enterprises must mitigate the identified risk and then maintain compliance through ongoing compliance and risk management activities. Enterprises should establish a corrective action plan (CAP) to appropriately address the discovered risk. If an enterprise is audited, the supervisory authority will most likely check to see not only if the enterprise performed a DPIA, but also if the enterprise performed the documented CAP. The supervisory authority asks to see the enterprise timeline for addressing or mitigating each of the DPIA findings, and how it is monitoring progress. Documentation is critical—if the enterprise does not document a GDPR-required component, then, basically, from an auditor or regulator perspective, the enterprise did not do it.

# Acknowledgments

ISACA would like to recognize:

## Lead Developer

**Rebecca Herold**
CISA, CISM, CISSP, FIP, CIPT, CIPM, CIPP/US, FLMI, SIMBUS, LLC and The Privacy Professor, USA

## Expert Reviewers

**Alan Lee**
CISA, CISM, CISSP, CIPT, ACA, HKICPA, EY, Hong Kong

**Vilius Benetis, Ph.D.**
CISA, CRISC, Director at NRD Cyber Security, Lithuania

## ISACA Board of Directors

**Theresa Grafenstine**
CISA, CRISC, CGEIT, CGAP, CGMA, CIA, CISSP, CPA, U.S. House of Representatives, USA, Chair

**Robert Clyde**
CISM, Clyde Consulting LLC, USA, Vice-Chair

**Brennan Baybeck**
CISA, CRISC, CISM, CISSP, Oracle Corporation, USA, Director

**Zubin Chagpar**
CISA, CISM, PMP, Amazon Web Services, UK, Director

**Peter Christiaans**
CISA, CRISC, CISM, PMP, Deloitte Consulting LLP, USA, Director

**Hironori Goto**
CISA, CRISC, CISM, CGEIT, ABCP, Five-I, LLC, Japan, Director

**Mike Hughes**
CISA, CRISC, CGEIT, Haines Watts, UK, Director

**Leonard Ong**
CISA, CRISC, CISM, CGEIT, CPP, CFE, PMP, CIPM, CIPT, CISSP ISSMP-ISSAP, CSSLP, CITBCM, GCIA, GCIH, GSNA, GCFA, Merck & Co., Inc., Singapore, Director

**R.V. Raghu**
CISA, CRISC, Versatilist Consulting India Pvt. Ltd., India, Director

**Jo Stewart-Rattray**
CISA, CRISC, CISM, CGEIT, FACS CP, BRM Holdich, Australia, Director

**Ted Wolff**
CISA, Vanguard, Inc., USA, Director

**Tichaona Zororo**
CISA, CRISC, CISM, CGEIT, COBIT 5 Certified Assessor, CIA, CRMA, EGIT | Enterprise Governance of IT (Pty) Ltd, South Africa, Director

**Christos K. Dimitriadis, Ph.D.**
CISA, CRISC, CISM, Intralot, S.A., Greece, Past Chair

**Robert E Stroud**
CRISC, CGEIT, Forrester Research, Inc., USA, Past Chair

**Tony Hayes**
CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Past Chair

**Matt Loeb**
CGEIT, FASAE, CAE, ISACA, USA, Director

# About ISACA

ISACA® (isaca.org) helps professionals around the globe realize the positive potential of technology in an evolving digital world. By offering industry-leading knowledge, standards, credentialing and education, ISACA enables professionals to apply technology in ways that instill confidence, address threats, drive innovation and create positive momentum for their organizations. Established in 1969, ISACA is a global association serving more than 500,000 engaged professionals in 188 countries. ISACA is the creator of the COBIT® framework, which helps organizations effectively govern and manage their information and technology. Through its Cybersecurity Nexus™ (CSX), ISACA helps organizations develop skilled cyber workforces and enables individuals to grow and advance their cyber careers.



ISACA®

3701 Algonquin Road, Suite 1010
Rolling Meadows, Il 60008 USA

**Phone:** +1.847.660.5505

**Fax:** +1.847.253.1755

**Support:** support.isaca.org

**Web:** www.isaca.org

**Provide Feedback:**
www.isaca.org/GDPR-DPIA

**Participate in the ISACA Knowledge Center:**
www.isaca.org/knowledge-center

**Follow ISACA on Twitter:**
www.twitter.com/ISACANews

**Join ISACA on LinkedIn:**
www.linkd.in/ISACAOfficial

**Like ISACA on Facebook:**
www.facebook.com/ISACAHQ