SCC

UNDERSTANDING GDPR

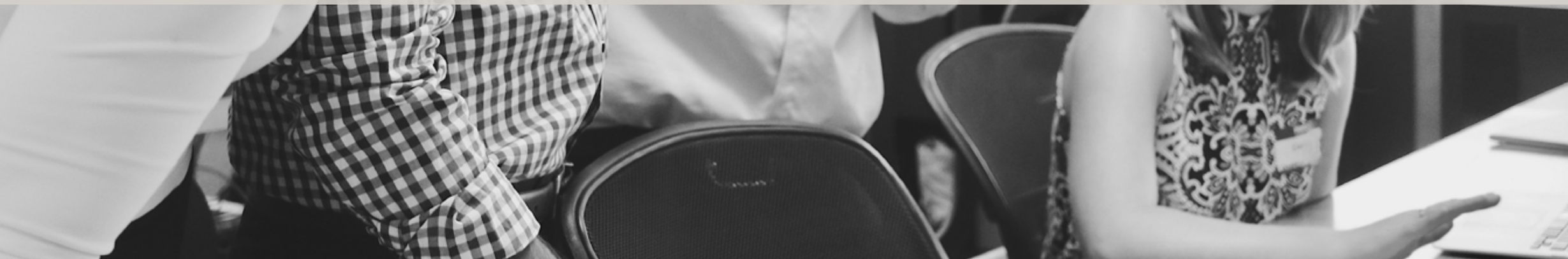
The role of standards in compliance

Standards Council of Canada

Open a world of possibilities.

Canada

The Standards Council of Canada would like to thank the members of the Canadian Advisory Committee on GDPR (CAC-GDPR) for sharing their expertise and for their contribution to this document.



DOCUMENT OBJECTIVE

The Standards Council of Canada (SCC) developed this guidance document to introduce Canadian organizations to the General Data Protection Regulation (GDPR) and to recommend standardization strategies that can facilitate the compliance process. This regulation established by the European Union (EU) has worldwide impact and may have significant implications for Canadian organizations.

Accordingly, this document explains how standardization may facilitate compliance with the GDPR. The information provided here will help organizations take the first steps on their path to compliance and guide them on the use of relevant standards. However, it is important to note that the GDPR is a complex regulation and complying to standards will not be sufficient to comply with the GDPR.

THE DOCUMENT PROVIDES:

- Interpretation of key GDPR Articles;
- Compliance examples;
- Examples of industries that are impacted by the GDPR;
- Standards that may help in understanding and complying with the GDPR;
- A list of recommended next steps;
- An annex containing a summary table which can be used as a quick reference tool for easy access to succinct information on the GDPR.

NOTE 1: This guidance document is intended for organizations, but may be used by the general public for information purposes.

NOTE 2: The text of this guidance document is based on the GDPR. Other interpretations are possible.

NOTE 3: Local laws and various data protection authorities may be responsible for enforcement or compliance related to GDPR.

NOTE 4: The adoption of any particular standard is optional, but generally encouraged, to achieve compliance with GDPR.

WHAT IS THE GENERAL DATA PROTECTION REGULATION?

The GDPR came into effect on May 25, 2018, to harmonize data protection laws across the EU. Enforced by the Data Protection Authorities (DPAs) in each EU Member State, the GDPR applies to organizations located within the EU as well as all organizations — regardless of location — that process or hold the personal data of data subjects residing in the EU. Canadian organizations must adhere to the GDPR if they offer goods or services to, or monitor the behaviour of, EU data subjects. Furthermore, Canadian organizations that process or transfer personal data of an individual of any citizenship, including Canadian, in the EU may need to comply with the regulation. Failure to comply with the GDPR can result in costly fines.

The GDPR requires the European Commission to monitor data protection laws in countries beyond the EU, including Canada. Only when a country's protections are deemed adequate can personal data flow from the EU to that country without additional safeguards being applied. The Canadian Government reports regularly to the European Commission to maintain Canada's existing adequacy status. However, as the result of a decision by the Court of Justice of the European Union (CJEU) in July of 2020, EU companies that wish to transfer personal data to data importers in other countries must first ascertain if the legal regime of the receiving country undermines the data importer's ability to adequately protect personal data. The CJEU gave a clear message that the free flow of personal data can take place only if the receiving country provides adequate protection for EU citizens' rights over their own data; and, if not, the EU organization is prohibited from giving access to the personal information. The CJEU decision means that EU data controllers must determine if the personal information they send outside the EU will be able to be adequately safeguarded in the destination countries.

WHAT ARE STANDARDS?

Standards are published specifications that ensure the reliability of materials, products, processes, and services. When used consistently, standards can ensure that materials, products, processes, and services are fit for their purpose. Standards are established by consensus and approved by a recognized body, such as SCC. Standards are based on consolidated subject matter expertise to promote optimum community benefits. In sum, standards define a benchmark for the design and development of innovations, and support domestic and international regulatory compliance. In addition, published standards may be accompanied by certification and accreditation programmes that facilitate international market access and regulatory compliance.

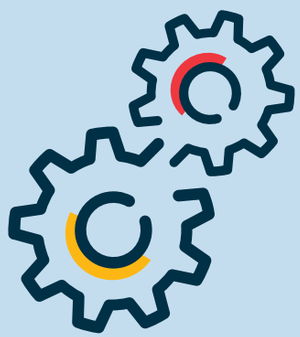
How Can Standards Help with the GDPR Compliance?
To keep up with technological advancements, changes to standards generally occur on a regular basis allowing organizations to adjust their compliance activities. Standardization can support the ability of Canadian organizations to comply with the GDPR by providing guidelines, methods, and procedures for meeting requirements set out in the GDPR. An array of voluntary standards has been and is being developed to enhance best practices in data privacy, cybersecurity, information and technology protection, and more. Although these standards are not directly referenced in the GDPR, they do provide a strong foundation to enable Canadian organizations to comply with the GDPR.

THE STANDARDS COUNCIL OF CANADA

Established in 1970 as a federal Crown corporation, the Standards Council of Canada (SCC) is Canada's voice on standards and accreditation on the national and international stage. SCC works closely with a vast network of partners to promote the development of effective and efficient standards that protect the health, safety, and well-being of Canadians while helping businesses prosper.

As Canada's leading accreditation organization, SCC creates market confidence at home and abroad by ensuring that conformity assessment bodies meet the highest national and international standards. SCC advances Canada's interest on the international scene as a member of the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) by connecting thousands of people to global networks and resources, opening a world of possibilities for Canadians and businesses.

For more information, visit https://www.scc.ca



KEY GDPR DEFINITIONS

TERRITORIAL SCOPE

The GDPR concerns the personal data of EU residents, regardless whether it is processed or stored within or outside the EU. The GDPR applies to organizations that (a) have an establishment in the EU; or (b) engage in data processing activities that relate to offering goods or services to EU residents; or (c) monitor the behaviour of EU residents within the EU, which may include tracking internet activity for behavioural advertising purposes. The GDPR applies to all non-European organizations which process personal data relating to EU residents, regardless of the organization's location.

(GDPR: Article 3, Recitals 22, 23, 24, 25)

DATA SUBJECT

A data subject is any natural person who can be identified via a number of identifiers such as a name, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity, either directly or indirectly. In other words, a data subject is a human being about whom and from whom an organization collects personal information.

(GDPR: Article 4, Recitals 15, 24, 26, 28, 29, 30, 31, 34, 35, 36, 37)

PERSONAL DATA

Personal data, often called "personal information" or "personally identifiable information", is any information that relates to an individual. This information can be provided by or collected from the individual, or created as a result of use or processing.

(GDPR: Article 4, Recitals 15, 24, 26, 28, 29, 30, 31, 34, 35, 36, 37)

DATA CONTROLLER

The data controller is the organization that decides what data will be collected, processed, and stored. The data controller is also responsible for the methods used for such collection, processing, and storage, as well as access, security, and retention. Included in this role is the decision on which third party organizations (processors) may be used.

(GDPR: Article 4, Recitals 15, 24, 26, 28, 29, 30, 31, 34, 35, 36, 37)

DATA PROCESSING

Data processing is any action executed on given data or set of personal data, which includes manipulating, categorizing, or running mathematical operations on the data.

(GDPR: Article 4, Recitals 15, 24, 26, 28, 29, 30, 31, 34, 35, 36, 37)

DATA PROCESSOR

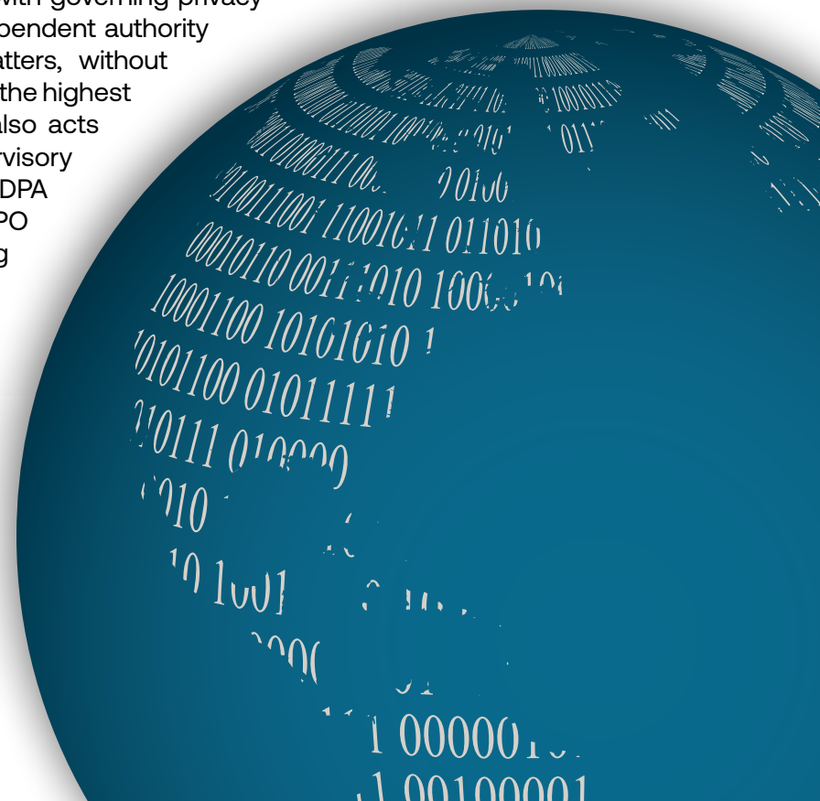
A data processor is an individual or organization that processes personal data at the direction of the data controller. A data processor does not own the personal information or control the purposes for processing. It is possible for an organization to be both a data controller and a data processor.

(GDPR: Article 4, Recitals 15, 24, 26, 28, 29, 30, 31, 34, 35, 36, 37)

DATA PROTECTION OFFICER

A data protection officer (DPO) is responsible to ensure that an organization complies with governing privacy laws. The DPO must have independent authority to execute on all privacy matters, without interference, and must report to the highest management level. The DPO also acts as a contact point for the supervisory DPA and co-operates with the DPA as needed. In addition, the DPO is responsible for providing guidance on all privacy matters, ensuring adequate training is in place, and assessing and reporting risks.

(GDPR: Article 37, 38, 39 Recitals 97)



GDPR KEY PRINCIPLES

PROCESSING AND ACCOUNTABILITY

The data collected shall be limited to only what is necessary, clearly identified to the data subject, and handled in a way that protects the safety and privacy of that information in a way that is adequate and proportionate to the sensitivity of the information.

(GDPR: Article 5, Recital 39)

LAWFULNESS

Processing of data is considered lawful if it is done with consent of the person about whom the data relates; if it is necessary to the function of the organizations collecting it; or if there is a valid legal reason to do so.

(GDPR: Article 6, Recitals 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 171)

CONSENT

Where applicable, personal data may only be collected, processed, or disclosed if the data subject has provided consent. The consent must be provided plainly, willingly and must be the result of an informed decision. Personal data may be processed where it is necessary for the controller's legitimate interests, and if it does not override the individual's fundamental rights and freedoms. Consent may be withdrawn by the data subject at any time.

(GDPR: Article 7, Recitals 32, 33, 42, 43)

CHILDREN'S CONSENT

The GDPR consent applies to data subjects over the age of 16. If a person is under the age of 16, the organization must obtain consent from the child's parent or guardian before any personal information about the child may be collected, processed, stored, or disclosed.

(GDPR: Article 8, Recital 38)

SPECIAL CATEGORIES

Processing of highly sensitive data is prohibited unless specifically consented by the data subject or other unique circumstances apply. Data that fall into the special categories include health data, biometrics, and data pertaining to a subject's race, sexual orientation, religious or philosophical belief, ethnicity, political view, and trade union membership.

(GDPR: Article 9, Recitals 46, 51, 52, 53, 54, 55, 56)

RELEVANT INTERNATIONAL STANDARDS

ISO/IEC 15944-5:2008 INFORMATION TECHNOLOGY — BUSINESS OPERATIONAL VIEW — PART 5: IDENTIFICATION AND REFERENCING OF REQUIREMENTS OF JURISDICTIONAL DOMAINS AS SOURCES OF EXTERNAL CONSTRAINTS | This standard aims to facilitate the establishment of an electronic business architecture in accordance with external requirements and restrictions such as jurisdictional domain. This document will help organizations adopt the GDPR in their practices.

ISO/IEC 15944-12:2020 INFORMATION TECHNOLOGY — BUSINESS OPERATIONAL VIEW — PART 12: PRIVACY PROTECTION REQUIREMENTS (PPR) ON INFORMATION LIFE CYCLE MANAGEMENT (ILCM) AND EDI OF PERSONAL INFORMATION (PI) | This standard provides a framework to identify external requirements and restrictions related to personal data for recorded information in business transactions. The best practice offer in this document can enhance the implementation of technical solutions to comply with the GDPR.

ISO/IEC 19944-1: CLOUD COMPUTING — CLOUD SERVICES AND DEVICES: DATA FLOW, DATA CATEGORIES AND DATA USE — PART 1: FUNDAMENTALS (UNDER DEVELOPMENT) | This standard provides the foundation for categorizing data that crosses between customers and cloud providers. For instance, it includes categories such as health data, where the GDPR is highly applicable.

ISO/IEC WD 19944-2: CLOUD COMPUTING AND DISTRIBUTED PLATFORMS — DATA FLOW, DATA CATEGORIES AND DATA USE — PART 2: GUIDANCE ON APPLICATION AND EXTENSIBILITY (UNDER DEVELOPMENT) | This standard will provide guidance on how to apply 19944-1 and includes privacy-related examples.

COMPLIANCE EXAMPLES

HOW THE GDPR APPLIES TO CANADIAN VENDORS

The GDPR is designed to protect the individual rights of EU residents and applies to European organizations, businesses that have offices in Europe, and individuals who reside in any of the EU countries. As a Canadian organization, you might think the GDPR only applies if you deal globally or have European customers; however, there are other cases to consider, such as the case for vendors.

Part of the regulation stipulates that GDPR-compliant organizations must use vendors whose processing activities are GDPR-compliant. In other words, EU organizations that make products or offer business-to-business services must purchase from vendors whose products and services meet the GDPR obligations. Depending on the level of sensitivity of the data that is handled, a data protection agreement may be signed to safeguard personal information. In other cases, a vendor agreement might be used, and would include verification that appropriate privacy and security measures are in place, and assurance that the vendor has an adequate mitigation strategy in place which, among other things, includes the timing and process for notifying customers if a data or security breach occurs.

EXAMPLES

1. A bookkeeping company has acquired a Canadian law firm as a new customer. The law firm has clients in the EU, and collects their personal and sensitive data, including financial statements, and confidential and privileged legal information. The law firm provides detailed receipts and invoices to the bookkeeping company so that it can carry out its work. In this case, the law firm must be GDPR-compliant for its EU clients, and the bookkeeping company must ensure that it processes their customer's data using a GDPR-compliant system to respect the law firm's compliance with the GDPR.

2. A tech company has created an application that acts as an online booking system, which is designed for use by anyone from personal trainers to plumbers to hairdressers. The system collects personal data such as clients' names and phone numbers. One of the customers is a Canadian fitness centre that has branches in the EU, and must therefore be GDPR-compliant. In addition, the vendor, in this case the tech company, must have a GDPR-compliant system to process the Canadian fitness centre's data.

HOW DOES THE GDPR AFFECT DIFFERENT INDUSTRIES?

The GDPR might apply to Canadian organizations even if they do not operate in the EU because the regulation covers personal data about EU citizens and residents regardless of where they are located. It can be difficult to know whether an individual is an EU citizen or resident when, for example, personal data is collected via website visits or call centres. When collecting personal information — whether digital or hard-copy — organizations must disclose what personal data they wish to collect, explain the purpose for collecting it, and include opt-in/opt-out options for collecting the information and before placing website cookies.

HEALTH CARE AND LIFE SCIENCES

A major impact of the GDPR on health care and life sciences organizations relates to explicit consent needed before collecting health, genetic, clinical trial, or biometric data. GDPR has restrictions on the collection of special category data which, because of its very nature, can pose a risk to individuals. Special category data includes ethnicity, religion, photos, video, fingerprints and other biometrics, and health data. Pseudonymization, de-identification, encryption, and other privacy protection mechanisms for clinical data is highly encouraged. Medical and life sciences organizations must also consider how to adequately safeguard the patient information, test results, medical images, and other data contained in and created by medical internet of things devices.

Compliance Examples: A multinational pharmaceutical corporation headquartered in Canada that conducts clinical trials in EU member states; a company that develops mobile health applications for wellness and chronic disease; a medical device manufacturer whose products provide real-time monitoring of patient vital signs.

CONSUMER RETAIL

The GDPR protects an individual's right to deny use of their data, and that has a major impact on the retail sector which must obtain consumers' consent to collect, process, or share their personal data. This protection affects retailers that rely on customer data for marketing and sales activities.

Compliance Examples: A company website with international traffic that uses cookies to collect personal information; a business that uses an existing or purchased database to send targeted marketing to EU residents.

INFORMATION SYSTEMS

The GDPR imposes obligations in relation to the information systems used by data processors and data protection. Under the GDPR, data processors must only process data in accordance with GDPR and controller requirements. They cannot appoint a sub-processor of the client's data without prior written consent of the processor.

Compliance Examples: A Canadian data centre that stores data on behalf of their customers; a cloud-based learning management system or an enterprise customer relationship management service that provides the use of its platform to customers who may collect personal data from platform users.

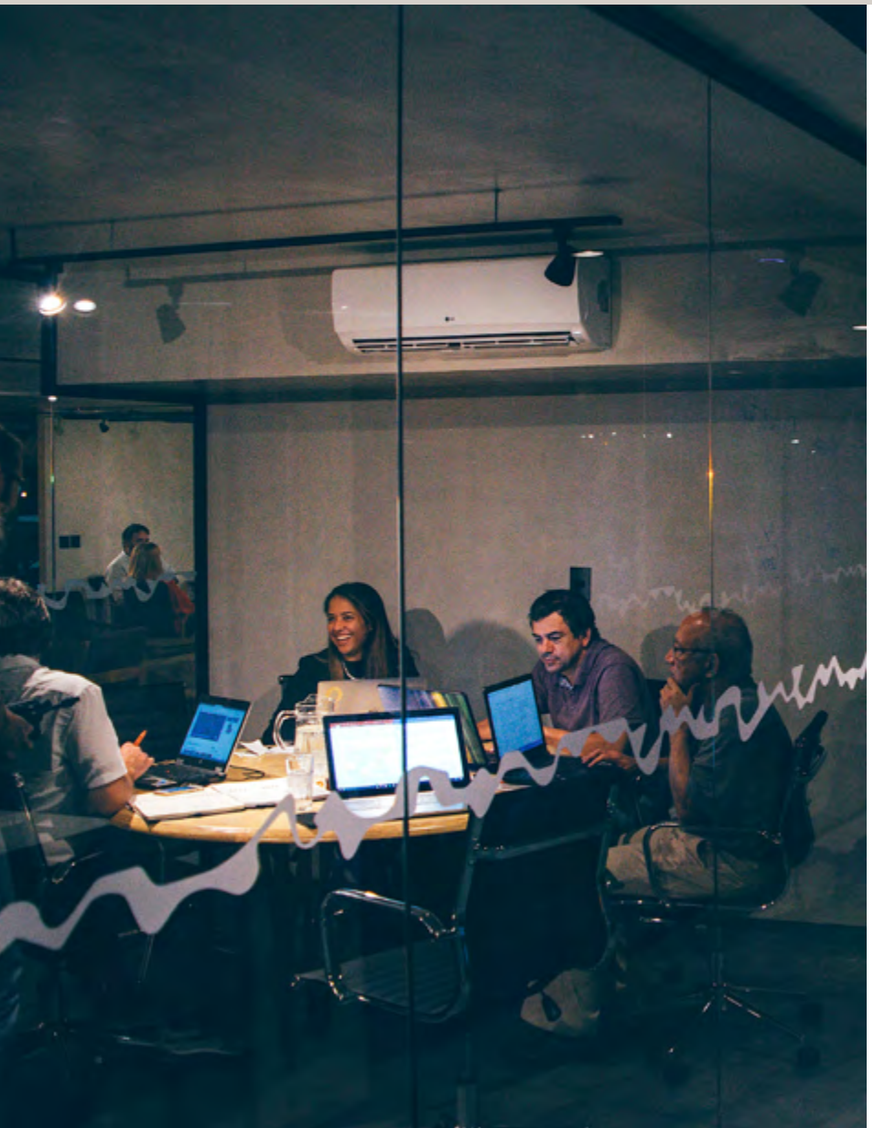
EDUCATION

A major impact of the GDPR on this sector relates to special category data and who has access to that data. The GDPR imposes restrictions on collecting special category data which, because of its very nature, can pose a risk to individuals. For instance, information about dietary restrictions may be collected or inferred that can reveal religious beliefs. Furthermore, collecting personal data from students under the age of 16 requires parental consent.

Compliance Examples: Canadian universities with EU students enrolled; faculty members collaborating on research projects with colleagues in the EU; public schools that collect information from EU students or their parents.

RIGHTS, OBLIGATIONS AND REMEDIES

Rights, obligations, and remedies under GDPR are quite extensive. The GDPR views privacy as a fundamental human right and, therefore, provides significant rights to data subjects and allows individuals much greater control over their data than is available under legislation elsewhere, including Canada. In addition, organizations that collect personal information have noteworthy obligations and liabilities to protect personal information.



SUBSTANTIVE RIGHTS OF DATA SUBJECTS

THE RIGHT TO BE INFORMED | The organization must inform the data subject about their rights in a way that is easy to access, clear to understand, and complete.

(GDPR: Articles 13, 14, Recitals 60, 61, 62)

THE RIGHT OF ACCESS | The data subject has the right to access all personal data held about them by an organization, including the way it is being processed.

(GDPR: Article 15, Recitals 63, 64)

THE RIGHT TO RECTIFICATION | The data subject has the right to correct any data about themselves that an organization is maintaining.

(GDPR: Article 16, Recital 65)

THE RIGHT TO ERASURE (RIGHT TO BE FORGOTTEN) | The data subject has the right to be fully removed from a system in a way that maintains no personal data. Please note that this provision is not absolute, and is subject to exceptions.

(GDPR: Articles 17, Recitals 65, 66)

THE RIGHT TO RESTRICT PROCESSING | The data subject has the right to ask an organization to cease processing their data. Unlike the right to erasure, the company may retain the subject's data, but they must not process it in any way.

(GDPR: Article 18, Recital 67)

THE RIGHT TO DATA PORTABILITY | The data subject has the right to receive their data in a way that is readable and easy to transfer to another organization for processing.

(GDPR: Article 20, Recital 68)

THE RIGHT TO OBJECT | The data subject has the right to refuse processing by third parties for the purpose of direct marketing (advertising) or research.

(GDPR: Article 21, Recitals 69, 70)

RIGHTS RELATED TO AUTOMATED DECISION MAKING AND PROFILING | The data subject has the right not to have decisions made about them by only automated systems or artificial intelligence. Please note that this provision is not absolute and is subject to exceptions.

(GDPR: Article 22, Recitals 71, 72, 91)

SUBSTANTIVE OBLIGATIONS OF ORGANIZATIONS

DATA CONTROLLER – RESPONSIBILITY | The controller is responsible for implementing sufficient technical and organizational measures to protect the privacy of the data subject and their information in a manner that is proportional to the sensitivity of the personal data.

(GDPR: Article 24, Recitals 74, 75, 76, 77)

DATA PROTECTION BY DESIGN AND BY DEFAULT | The principles of privacy by design and privacy by default shall be applied to ensure that the foundation of the product or service meets both privacy and security needs.

(GDPR: Article 25, Recital 78)

JOINT CONTROLLER | If two controllers are responsible for determining the use of data, the controllers then become joint controllers and must agree who is responsible for fulfilling the data subject's rights when requested.

(GDPR: Article 26, Recital 79)

REPRESENTATIVES OF CONTROLLERS NOT IN THE EU | If neither the controller nor the processor is in the EU, they must assign a representative that does reside within the EU. This assignment must be established in writing, and the relevant DPA must be notified.

(GDPR: Article 27, Recital 80)

PROCESSOR | For a controller to be compliant, all processors chosen must ensure that the processing task meets the GDPR obligations.

(GDPR: Article 28, Recital 81)

PROCESSING | The processor shall only process the data for which they have been tasked by the controller or, if required, by Union or Member State law.

(GDPR: Article 29, Recital none)

RECORDS OF PROCESSING | Controllers must retain a record that includes information about their DPO and representatives. They must also list what data is being processed, including the legal basis for processing, the categorization of that data, and whether or not it is personal information.

(GDPR: Article 30, Recitals 13, 82)

COOPERATION WITH SUPERVISORY AUTHORITIES | The controller and the processor are required to cooperate with the relevant DPA on request.

(GDPR: Article 31, Recital 82)

RELEVANT INTERNATIONAL STANDARDS

ISO/IEC 20546:2019 INFORMATION TECHNOLOGY — BIG DATA — OVERVIEW AND VOCABULARY | This standard determines a clear and common language to facilitate the understanding of different concepts around big data, which can help compliance with the GDPR.

ISO/IEC 20889:2018 PRIVACY ENHANCING DATA DE-IDENTIFICATION TERMINOLOGY AND CLASSIFICATION OF TECHNIQUES | This standard elaborates on the use and importance of de-identification in accordance to the privacy principles established in ISO/IEC 29100. This standard can help to enhance the protection of personal data.

ISO/IEC 22624:2020 INFORMATION TECHNOLOGY — CLOUD COMPUTING — TAXONOMY BASED DATA HANDLING FOR CLOUD SERVICES | This standard incorporates further data classification and geo-location information, specifically highlighting where regulation such as the GDPR needs to be considered.

ISO/IEC TR 22678:2019 INFORMATION TECHNOLOGY — CLOUD COMPUTING — GUIDANCE FOR POLICY DEVELOPMENT | This high level executive standard highlights that policies may need to be analyzed and potentially changed, clarified, or interpreted. Policies and interpretations around the GDPR might be required to have a clear position.

SUBSTANTIVE OBLIGATIONS OF ORGANIZATIONS

SECURITY OF PROCESSING | The controller and processor are responsible for ensuring they have implemented suitable technical and organizational procedures to ensure the security of their systems to protect the data. This obligation extends to ensuring adequate controls are in place to limit physical access.

(GDPR: Article 32, Recitals 75, 76, 77, 78, 79, 83)

DATA BREACH NOTIFICATION (TO AUTHORITY) | If a security or data breach occurs, the controller must notify the supervising authority within 72 hours of becoming aware of the breach. The controller does not have to notify the authorities if the risk of harm to the individual is low or non-existent. In addition, any processor that experiences a breach must inform the controller without delay.

(GDPR: Article 33, Recitals 85, 87, 88)

DATA BREACH NOTIFICATION (TO DATA SUBJECT) | If a security or data breach could cause a high risk of harm to a data subject, the controller must inform the individual. The notification must include an explanation of what data was compromised, what the company is doing to control the situation, and clear instructions for the data subject as to what they might need to do to protect themselves and their data.

(GDPR: Article 34, Recitals 86, 87, 88)

DATA PROTECTION IMPACT ASSESSMENT/PRIOR CONSULTATIONS | Controllers must conduct a Data Protection Impact Assessment (DPIA) on their products and services to identify if personal information will be involved, and whether or how the privacy of that information might be affected on processing that is likely to result in high risk for data subject. DPIAs are an essential risk management tool that provides an opportunity to map systems and data flows, and to identify, consider, measure, and mitigate or eliminate risk to privacy.

(GDPR: Articles 35, 36, Recitals 75, 84, 89, 90, 91, 92, 93, 94, 95, 96)

DESIGNATION/POSITION/TASKS OF DATA PROTECTION OFFICER | An organization that processes information in relation to monitoring data subjects, or which has processing done by a public body, must appoint a DPO. The DPO is responsible for communications between the controller, the processor, and the supervising authority. The DPO oversees the organization's proper compliance with the GDPR.

(GDPR: Articles 37, 38, 39, Recital 97)

RELEVANT INTERNATIONAL STANDARDS

ISO/IEC CD 23751 INFORMATION TECHNOLOGY — CLOUD COMPUTING AND DISTRIBUTED PLATFORMS — DATA SHARING AGREEMENT (DSA) FRAMEWORK (UNDER DEVELOPMENT) | This standard will explore how data sharing agreements can be established. This permitted sharing concept can impact how the GDPR is applied.

ISO/IEC 27001:2013 INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY MANAGEMENT SYSTEMS — REQUIREMENTS | This popular standard provides a robust framework for the establishment of an information security management system (ISMS), which can help prevent data breaches and facilitate GDPR compliance.

ISO/IEC 27002:2013 INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS | This standard provides guidance on how to apply 27001 and help in selecting the right controls for the establishment of an ISMS.

ISO/IEC 27018:2019 INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — CODE OF PRACTICE FOR PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII) IN PUBLIC CLOUDS ACTING AS PII PROCESSORS | This standard establishes a framework to protect PII in public cloud computing in accordance with ISO/IEC 29100 and based on ISO/IEC 27002. This enhanced protection for PII can help improve the protection of personal data, an essential element of the GDPR.

REMEDIES FOR DATA SUBJECTS

RIGHT TO LODGE A COMPLAINT | Data subjects have the right to file a complaint with the supervising authority if they think that their data has been handled in any way that breaches their rights under the GDPR.

(GDPR: Article 77, Recital 141)

RIGHT TO AN EFFECTIVE REMEDY AGAINST A CONTROLLER OR PROCESSOR | Data subjects have the right to a judicial remedy if their personal information has been used in a way that infringes their rights as the data subject.

(GDPR: Article 79, Recitals 141, 145)

PENALTIES

ADMINISTRATIVE FINES | Fines are based on damage to data subjects, the number of data subjects affected, and the degree of due diligence taken by the controller or processor. Fines can be up to 20 million Euros or between 2% and 4% of global annual gross revenue from the previous year, depending on the violation.

(GDPR: Article 83, Recitals 148, 149, 150, 151, 152)

PENALTIES | Member states are responsible for setting the rules for any additional penalties they might wish to impose on controllers and processors.

(GDPR: Article 84, Recitals 149, 150, 151, 152)

LIABILITIES

RIGHT TO COMPENSATION AND LIABILITY Data subjects have the right to receive compensation if they have suffered material (e.g., financial loss) or non-material harm (e.g., reputational damage) due to infringement of the GDPR obligations by a controller or, in specific cases, a processor.

(GDPR: Article 82, Recitals 146, 147)

RELEVANT INTERNATIONAL STANDARDS

ISO/IEC 27701:2019 SECURITY TECHNIQUES — EXTENSION TO ISO/IEC 27001 AND ISO/IEC 27002 FOR PRIVACY INFORMATION MANAGEMENT — REQUIREMENTS AND GUIDELINES | This standard is an addition to ISO/IEC27001 and ISO/IEC27002 and provides additional guidance to maintain a privacy information management system.

ISO/IEC 29100:2011 INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — PRIVACY FRAMEWORK | This document provides a personally identifiable information security framework for information and communication technology to improve the handling of personal data. This can provide additional support for the GDPR compliance process.

ISO/IEC 29151:2017 INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — CODE OF PRACTICE FOR PERSONALLY IDENTIFIABLE INFORMATION PROTECTION | Based on ISO/IEC 27002, this standard highlights guidance for the application of controls to limit exposure to data breaches, a key objective of the GDPR.

ISO/IEC 29184:2020 INFORMATION TECHNOLOGY — ONLINE PRIVACY NOTICES AND CONSENT | This standard provides a foundation for informed customer consent of data usage and closely aligns with the GDPR requirements.

ISO/AWI 31700 CONSUMER PROTECTION — PRIVACY BY DESIGN FOR CONSUMER GOODS AND SERVICES (UNDER DEVELOPMENT) | This consumer privacy standard provides a requirements roadmap for organizations to design and implement privacy features and controls into their products. It addresses the privacy issues raised by the GDPR.

ISO/IEC 38500:2015 INFORMATION TECHNOLOGY — GOVERNANCE OF IT FOR THE ORGANIZATION | This standard provides a governance model to establish an efficient IT infrastructure, which can facilitate the transition towards a GDPR-compliant model.

ISO/IEC 38505-1:2017 INFORMATION TECHNOLOGY — GOVERNANCE OF IT — GOVERNANCE OF DATA — PART 1: APPLICATION OF ISO/IEC 38500 TO THE GOVERNANCE OF DATA | This standard provides guidance for organizations on how to apply ISO/IEC 38500.

NEXT STEPS

1) ADOPTING A DATA PROTECTION BY DESIGN AND DEFAULT FRAMEWORK

Data protection incorporates the values and requirements of information management, information security, data privacy, and data governance. Best practices and continuous improvement of data protection measures are strongly encouraged. Data protection compliance varies by industry and jurisdiction, and by the type(s) of information collected and used by an organization, but all organizations are wise to comply — whether to meet legislative, regulatory, or customer expectations.

2) PERFORMING A DATA PROTECTION IMPACT ASSESSMENT

Protecting personal information and the rights of individuals is fundamental to the GDPR. Organizations should conduct a DPIA — before designing, developing, acquiring, or implementing any process, product, or system — to evaluate how personal data is collected, accessed, stored, transferred, and disposed of throughout its entire lifecycle. Organizations should also consider the legal bases, such as consent, for data processing or control. The DPIA must also provide a system map and a data map that tracks the input, access, and storage of data through the system. Please note that a DPIA must be performed when the processing may present high risk to the data subject.

3) DEVELOPING A DATA PROCESSING AGREEMENT

Most organizations work with third parties to process and control data. This creates ecosystems of data that require data processing agreements to govern the data protection rights and responsibilities among the members of that ecosystem. Agreements must be clear and unambiguous, and their language must be consistent with that of the GDPR. Consulting an experienced and well-qualified privacy professional, or a lawyer who has expertise in privacy, is advisable.

4) APPOINTING A DATA PRIVACY OFFICER

Many organizations are required by the GDPR to have a DPO; other organizations may choose to have a DPO. A DPO is responsible for providing guidance and coordination on privacy matters at an organization. Ensure the DPO is properly qualified and that they possess the skills, knowledge, and experience necessary to help an organization navigate its way through increasingly complex national and global privacy, access, and data protection challenges.

5) LOOKING FOR COMPLIANCE OPTIONS

In the spirit of protecting consumer data in a world of increasingly borderless commerce, complying with data privacy, data security, and related quality management systems is essential. Available compliance options include organizational self-certification, private certifications, and certification to international standards. (Note: Canada is a participating member of ISO PC 317, drafting the ISO standard that relates to the GDPR-based data protection requirements.)

6) RESPECTING CROSS-BORDER TRANSFER LAWS

Since 2001, Canada has enjoyed the enviable position of having been granted adequacy status by the EU, allowing personal data flow from the EU to Canada, recognizing that the Personal Information Protection and Electronic Documents Act (PIPEDA) offers a level of data protection equivalent to that provided to EU citizens. According to PIPEDA, “An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.” However, Canada’s privacy and access laws have not been updated to meet the GDPR standard yet, so it’s important to maintain vigilance in this area to ensure compliance with any change related to the adequacy status.

7) ENGAGE IN CONTINUOUS IMPROVEMENT

Best practices in compliance include a continuous improvement model, which is an opportunity for an organization to improve its products and governance practices, improve the privacy features of its products, and improve its overall relationship with consumers and regulators. Use of continuous improvement cycles is encouraged.

WE'RE HERE TO HELP

Helping Canadian businesses thrive through standardization is what we do.

The information provided herein is meant to foster your company's efforts towards GDPR compliance. For additional resources and to learn more about how standardization can help your company prosper, visit our website at www.scc.ca.

MAKE YOUR MARK AND CONTACT US TODAY

613-238-3222
innovation@scc.ca
www.scc.ca

ANNEX

KEY GDPR ARTICLES AND STANDARDS THAT CAN SUPPORT COMPLIANCE

This table summarizes the information from the previous sections. It is recommended to use this table as a quick reference tool for easy access to succinct information on the GDPR.

KEY GDPR ARTICLES	ARTICLES	RELEVANT RECITALS	DESCRIPTIONS *These descriptions are based on the GDPR and may differ from other interpretations.	RELEVANT INTERNATIONAL STANDARDS THAT CAN FACILITATE COMPLIANCE WITH THE GDPR
GENERAL PROVISION – SCOPE & DEFINITIONS				
1. Territorial Scope (Extraterritoriality)	3	22, 23, 24, 25	The GDPR concerns the personal data of EU residents, regardless whether it is processed or stored within or outside the EU. The GDPR applies to organizations that (a) have an establishment in the EU; or (b) engage in data processing activities that relate to offering goods or services to EU residents; or (c) monitor the behaviour of EU residents within the EU, which may include tracking internet activity for behavioural advertising purposes. The GDPR applies to all non-European organizations which process personal data relating to EU residents, regardless of the organization's location.	**ISO/IEC 15944-5:2008** Information technology — Business operational view — Part 5: Identification and referencing of requirements of jurisdictional domains as sources of external constraints **ISO/IEC 15944-12:2020** Information technology — Business operational view — Part 12: Privacy protection requirements (PPR) on information life cycle management (ILCM) and EDI of personal information (PI) **ISO/IEC 19944-1:** Cloud computing — Cloud services and devices: data flow, data categories and data use — Part 1: Fundamentals (Under Development) **ISO/IEC WD 19944-2:** Cloud computing and distributed platforms — Data flow, data categories and data use — Part 2: Guidance on application and extensibility (Under Development) **ISO/IEC 20546:2019** Information technology: Big data — Overview and vocabulary
2. Definitions	4	15, 24, 26, 28, 29, 30, 31, 34, 35, 36, 37		
a. Personal Data			Personal data, often called "personal information" or "personally identifiable information" is any information that relates to an individual. This information can be provided by or collected from the individual, or created as a result of use or processing.	
b. Data Processing			Data processing is any action executed on given data or set of personal data, which includes manipulating, categorizing, or running mathematical operations on the data.	
c. Data Subject			A data subject is any natural person who can be identified via a number of identifiers such as a name, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity, either directly or indirectly. In other words, a data subject is a human being about whom and from whom an organization collects personal information.	
d. Data Controller			The data controller is the organization that decides what data will be collected, processed, and stored. The data controller is also responsible for the methods used for such collection, processing, and storage, as well as access, security, and retention. Included in this role is the decision on which third party organizations (processors) may be used.	
e. Data Processor			A data processor is an individual or organization that processes personal data at the direction of the data controller. A data processor does not own the personal information or control the purposes for processing. It is possible for an organization to be both a data controller and a data processor.	

KEY GDPR ARTICLES	ARTICLES	RELEVANT RECITALS	DESCRIPTIONS *These descriptions are based on the GDPR and may differ from other interpretations.	RELEVANT INTERNATIONAL STANDARDS THAT CAN FACILITATE COMPLIANCE WITH THE GDPR
f. Data Protection Officer	37, 38, 39	97	A DPO is responsible to ensure that an organization complies with governing privacy laws. The DPO must have independent authority to execute on all privacy matters, without interference, and must report to the highest management level. The DPO also acts as a contact point for the supervisory DPA and co-operates with the DPA as needed. In addition, the DPO is responsible for providing guidance on all privacy matters, ensuring adequate training is in place, and assessing and reporting risks.	**ISO/IEC 20889:2018** Privacy enhancing data de-identification terminology and classification of techniques **ISO/IEC 22624:2020** Information technology — Cloud computing — Taxonomy based data handling for cloud services **ISO/IEC TR 22678:2019** Information technology — Cloud computing — Guidance for policy development **ISO/IEC CD 23751:** Information technology — Cloud computing and distributed platforms — Data sharing agreement (DSA) framework (Under development) **ISO/IEC 27001:2013** Information technology — Security techniques — Information security management systems — Requirements **ISO/IEC 27002:2013** Information technology — Security techniques — Code of practice for information security controls **ISO/IEC 27018:2019** Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
PRINCIPLES				
1. Processing and Accountability	5	39	The data collected shall be limited to only what is necessary, clearly identified to the data subject, and handled in a way that protects the safety and privacy of that information in a way that is adequate and proportionate to the sensitivity of the information.	
2. Lawfulness	6	39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 171	Processing of data is considered lawful if it is done with consent of the person about whom the data relates; if it is necessary to the function of the organizations collecting it; or if there is a valid legal reason to do so.	
3. Consent	7	32, 33, 42, 43	Where applicable, personal data may only be collected, processed, or disclosed if the data subject has provided consent. The consent must be provided plainly, willingly and must be the result of an informed decision. Personal data may be processed where it is necessary for the controller's legitimate interests, and if it does not override the individual's fundamental rights and freedoms. Consent may be withdrawn by the data subject at any time.	
4. Children's Consent	8	38	The GDPR consent applies to data subjects over the age of 16. If a person is under the age of 16, the organization must obtain consent from the child's parent or guardian before any personal information about the child may be collected, processed, stored or disclosed.	
5. Special Categories	9	46, 51, 52, 53, 54, 55, 56	Processing of highly sensitive data is prohibited unless specifically consented by the data subject or other unique circumstances apply. Data that fall into the special categories include health data, biometrics, and data pertaining to a subject's race, sexual orientation, religious or philosophical belief, ethnicity, political view, and trade union membership.	
SUBSTANTIVE RIGHTS OF DATA SUBJECTS				
1. The Right to Be Informed	13, 14	60, 61, 62	The organization must inform the data subject about their rights in a way that is easy to access, clear to understand, and complete.	
2. The Right of Access	15	63, 64	The data subject has the right to access all personal data held about them by an organization, including the way it is being processed.	

KEY GDPR ARTICLES	ARTICLES	RELEVANT RECITALS	DESCRIPTIONS *These descriptions are based on the GDPR and may differ from other interpretations.	RELEVANT INTERNATIONAL STANDARDS THAT CAN FACILITATE COMPLIANCE WITH THE GDPR
SUBSTANTIVE RIGHTS OF DATA SUBJECTS				
3. The Right to Rectification	16	65	The data subject has the right to correct any data about themselves that an organization is maintaining.	**ISO/IEC 27701:2019** Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines **ISO/IEC 29100:2011** Information technology — Security techniques — Privacy framework **ISO/IEC 29151:2017** Information technology — Security techniques — Code of practice for personally identifiable information protection **ISO/IEC 29184:2020** Information technology — Online privacy notices and consent **ISO/AWI 31700** Consumer protection — Privacy by design for consumer goods and services (Under development) **ISO/IEC 38500:2015** Information technology — Governance of IT for the organization **ISO/IEC 38505-1:2017** Information technology — Governance of IT — Governance of data — Part 1: Application of ISO/IEC 38500 to the governance of data
4. The Right to Erasure (Right to Be Forgotten)	17	65, 66	The data subject has the right to be completely removed from a system in a way that maintains no personally identifiable information.	
5. The Right to Restrict Processing	18	67	The data subject has the right to ask an organization to cease any processing on their data. Unlike the right to erasure the company may continue to keep the subject's data, but they cannot process it in any way.	
6. The Right to Data Portability	20	68	The data subject has the right to receive their data in a way that is readable and easy to transfer to a separate organization for processing.	
7. The Right to Object	21	69, 70	The data subject has the right to refuse processing by third party companies for the purpose of direct marketing (advertising) or research.	
8. Rights Related to Automated Decision Making and Profiling	22	71, 72, 91	The data subject has the right not to have decisions made about them by only automated systems or artificial intelligence.	
SUBSTANTIVE OBLIGATIONS OF ORGANIZATIONS				
1. Data Controller – Responsibility	24	74, 75, 76, 77	The controller is responsible for implementing sufficient technical and organizational measures to protect the privacy of the data subject and their information in a manner that is proportional to the sensitivity of the personal data.	
2. Data Protection by Design and by Default	25	78	The principles of privacy by design and by default shall be applied to ensure that the foundation of the product or service meets both privacy and security needs.	
3. Joint Controller	26	79	If two controllers are responsible for determining the use of data, the controllers then become joint controllers and must agree who is responsible for fulfilling the data subject's rights when requested.	

KEY GDPR ARTICLES	ARTICLES	RELEVANT RECITALS	DESCRIPTIONS *These descriptions are based on the GDPR and may differ from other interpretations.	RELEVANT INTERNATIONAL STANDARDS THAT CAN FACILITATE COMPLIANCE WITH THE GDPR
SUBSTANTIVE OBLIGATIONS OF ORGANIZATIONS				
4. Representatives of Controllers Not in the EU	27	80	If neither the controller nor the processor is in the EU, they must assign a representative that does reside within the EU. This assignment must be established in writing, and the relevant DPA must be notified.	
5. Processor	28	81	For a controller to be compliant, all processors chosen must ensure that the processing task meets the GDPR obligations.	
6. Processing	29	None	The processor shall only process the data for which they have been tasked by the controller or, if required, by Union or Member State law.	
7. Records of Processing	30	13, 82	Controllers must retain a record that includes information about their DPO and representatives. They must also list what data is being processed, including the legal basis for processing, the categorization of that data, and whether or not it is personal information.	
8. Cooperation with Supervisory Authorities	31	82	The controller and the processor are required to cooperate with the relevant DPA on request.	
9. Security of Processing	32	75, 76, 77, 78, 79, 83	The controller and processor are responsible for ensuring they have implemented suitable technical and organizational procedures to ensure the security of their systems to protect the data. This obligation extends to ensuring adequate controls are in place to limit physical access.	
10. Data Breach Notification (to Authority)	33	85, 87, 88	If a security or data breach occurs, the controller must notify the supervising authority within 72 hours of becoming aware of the breach. The controller does not have to notify the authorities if the risk of harm to the individual is low or non-existent. In addition, any processor that experiences a breach must inform the controller without delay.	
11. Data Breach Notification (to Data Subject)	34	86, 87, 88	If a security or data breach could cause a high risk of harm to a data subject, the controller must inform the individual. The notification must include an explanation of what data was compromised, what the company is doing to control the situation, and clear instructions for the data subject as to what they might need to do to protect themselves and their data.	
12. Data Protection Impact Assessment/Prior Consultations	35, 36	75, 84, 89, 90, 91, 92, 93, 94, 95, 96	Controllers must conduct a DPIA on their products and services to identify if personal information will be involved, and whether or how the privacy of that information might be affected on processing that is likely to result in high risk for data subject. DPIAs are an essential risk management tool that provides an opportunity to map systems and data flows, and to identify, consider, measure, and mitigate or eliminate risk to privacy.	

KEY GDPR ARTICLES	ARTICLES	RELEVANT RECITALS	DESCRIPTIONS *These descriptions are based on the GDPR and may differ from other interpretations.	RELEVANT INTERNATIONAL STANDARDS THAT CAN FACILITATE COMPLIANCE WITH THE GDPR
SUBSTANTIVE RIGHTS OF DATA SUBJECTS				
13. Designation/ Position/Tasks of Data Protection Officer	37, 38, 39	97	An organization that processes information in relation to monitoring data subjects, or which has processing done by a public body, must appoint a DPO. The DPO is responsible for communications between the controller, the processor, and the supervising authority. The DPO oversees the organization's proper compliance with the GDPR.	
ENFORCEMENT: REMEDIES, LIABILITIES & PENALTIES				
1. REMEDIES				
a. Right (for Data Subjects) to Lodge a Complaint	77	141	Data subjects have the right to file a complaint with the supervising authority if they think that their data has been handled in any way that breaches their rights under the GDPR.	
b. Right (for Data Subjects) to an Effective Remedy Against a Controller or Processor	79	141, 145	Data subjects have the right to a judicial remedy if their personal information has been used in a way that infringes their rights as the data subject.	
2. LIABILITIES				
a. Right (for Data Subjects) to Compensation and Liability	82	146, 147	Data subjects have the right to receive compensation if they have suffered material (e.g., financial loss) or non-material harm (e.g., reputational damage) due to infringement of the GDPR obligations by a controller or, in specific cases, a processor.	
3. PENALTIES				
a. Administrative Fines	83	148, 149, 150, 151, 152	Fines are based on damage to data subjects, the number of data subjects affected, and the degree of due diligence taken by the controller or processor. Fines can be up to 20 million Euros or between 2% and 4% of global annual gross revenue from the previous year, depending on the violation.	
b. Penalties	84	149, 150, 151, 152	Member states are responsible for setting the rules for any additional penalties they might wish to impose on controllers and processors.	