European Union (EU) General Data Protection Regulation (GDPR)

Do you handle EU residents' personal data? The GDPR update is coming May 25, 2018. Are you ready?

What do you need to do?

Governance and Accountability – An appropriate data management framework should be established (by senior management) to ensure compliance with regulatory requirements and enable continual improvement.

Each firm must decide if it is a data controller or a data processor. A data controller is an organization such as a retailer that collects personal data while selling products to EU data subjects, and also determines the purpose and methods for processing personal data. Marketing research firms can also be data controllers if functioning as primary data collectors. A data processor is an organization that processes personal data on behalf of a data controller, such as a marketing firm that sends emails to EU data subjects on behalf of a retailer. Marketing research firms may function as data processors if they are conducting marketing research studies from client-supplied lists. Because of the nature of marketing research studies, firms will find that they have the dual roles of the data controller and data processor.

Identify - Where in the whole organization including third-party providers are EU residents' personal data stored? Identification must take place, whether it's personal data at rest or personal data in motion.

Classify - What is the nature of the personal data? For what purpose is it being stored, processed, or serviced? Does any of the personal data belong to individuals under the age of 16? Is there documented proof of consent associated with the information? The individuals which the personal information belongs to must be aware that the company has the information, and for what purpose(s) the data are being used.

Protect – Where does the data reside? Other than your back-up, is the data in one location or multiple locations? A plan must be in place to protect the data at all locations, during processing and in transit. The plan may include consolidation, encryption, and defined segmentation to build specific controls. Access is limited to a need-to-know for business purposes only. Also, to maintain data integrity and demonstrate data control, members should build into their systems the ability to monitor and audit whoever is allowed access to EU residents' personal data.

How do you go about implementing protection?

Firms may implement their own plan or use an independent third party to implement the plan. The EU Regulation recognizes voluntary certifications from approved and accredited certification bodies as acceptable mechanisms for demonstrating compliance to GDPR (see Article 42). Members who choose to get an ISO-27001 certification must obtain it from ISO or an entity granted ISO/IEC17065 Certification by an EU state.

ISO 27001 - Information technology — Security techniques — Information security management systems-Requirements. The EU recognizes the ISO -27001 certification.

Personal data

Any piece of information that can be used to identify an EU resident, which includes the following:

- Name
- Photo
- Email address
- Financial account details
- Social network posts
- Medical information
- IP address
- ID number
- Biometrics
- DNA

GDPR (General Data Protection Regulation)	**PIPEDA (Personal Information Protection and Electronic Documents Act)**
Increased Territorial Scope (Extraterritorial - EU residents' data that are handled outside of the EU are covered)	Limited to Canada
Penalties - up to 4% of worldwide gross revenue, - or 20 million Euros, whichever is greater	Fines as set by the Privacy Commission Officer
Data Protection Officer (the Privacy Officer may be a suitable candidate for this role).	Privacy Officer – Principle 1 – Accountability Responsible for enforcing the ten principles
Consent in plain language.	Principle 3 – Consent.
The right to be forgotten - This is a new and important change.	Principle 4 - Limiting Collection, and Principle 5 - Limiting Use Disclosure and Retention. Do not keep information for longer than it is needed.
Privacy by Design.	PIPEDA Ten Principles
Breach Notification – The right of the individual to be notified.	PIPEDA Breach Notification reporting (fines up to $100,000 for failure to comply)
Right to Access	Principle 8 – Openness, and Principle 9- Right to Access Information.
Data Portability - Information must be presented in a machine-readable language to the individual	PIPEDA does not have a specific policy on portability. However, since the information is available for the individual to review, the steps to comply with this requirement may not be too onerous. Principle 9 – Individual Access.
Right to be Forgotten – Data Erasure – The data subject can have all past data erased, cease further dissemination and stop third-party processing of the data. Data controllers to compare subject rights to the "public interest in the availability of the data", EU GDPR Article 17.	Principle 5- Limiting Use, Disclosure, and Retention.
Note: GDPR's definition of personal data is quite broad; any information that can identify the individual. This also includes: Biometrics, Genetic Data, Internet Protocol (IP) address.	PIPEDA refers to Personally Identifiable Information (PII), e.g., name, address, phone number, employment information—any information that can be used to identify a person

KEY Changes

Here is a release from the EU GDPR on the major changes to the Regulations. Also, here is the link to the site; EU GDPR Key Changes

The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established. Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies; the key points of the GDPR as well as information on the impacts it will have on business can be found below.

Increased Territorial Scope (extra-territorial applicability)

Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. Previously, territorial applicability of the directive was ambiguous and referred to data process 'in context of an establishment'. This topic has arisen in a number of high profile court cases. GPDR makes its applicability very clear - it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. Non-Eu businesses processing the data of EU citizens will also have to appoint a representative in the EU.

Penalties

Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

Consent

The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Data Subject Rights

Breach Notification

Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

Right to Access

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

Right to be Forgotten

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

Data Portability

GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a '*commonly use and machine readable format*' and have the right to transmit that data to another controller.

Privacy by Design

Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. At it's core, privacy by design calls for the inclusion of data rotection from the onset of the designing of systems, rather than an addition. More specifically - *'The controller shall implement appropriate technical and organisational measures in an effective way. in order to meet the requirements of this Regulation and protect the rights of data subjects'.* Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

Data Protection Officers

Currently, controllers are required to notify their data processing activities with local DPAs, which, for multinationals, can be a bureaucratic nightmare with most Member States having different notification requirements. Under GDPR it will not be necessary to submit notifications / registrations to each local DPA of data processing activities, nor will it be a requirement to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there will be internal record keeping requirements, as further explained below, and DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular

and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. Importantly, the DPO:

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
- May be a staff member or an external service provider
- Contact details must be provided to the relevant DPA
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
- Must report directly to the highest level of management
- Must not carry out any other tasks that could results in a conflict of interest.