A BRAVE NEW WORLD: THE EU'S NEW DATA PROTECTION RULES

LETTE
LAWYERS - AVOCATS - RECHTSANWÄLTE

The EU's new General Data Protection Regulation (GDPR) will come into force on May 25, 2018, ushering in an era of heightened privacy protection for EU residents. The GDPR is intended to give EU residents greater control over their personal data and greater rights in the event of a data processing breach. Unlike its predecessor legislation, the Data Protection Directive, the GDPR is mandatory law that applies uniformly in all EU states. While this harmonization may be a benefit to companies doing business in the EU, it comes at the cost of more onerous compliance obligations and significant potential penalties.

One of the biggest changes is the expanded territorial application of the GDPR, as it applies to all companies processing the personal data of individuals ("data subjects") in the EU, regardless of a company's location. Specifically, it applies not only to organizations in the EU that process personal data (even if the processing occurs outside of the EU), but also to organizations located outside of the EU who (i) offer goods and services to EU residents, or (ii) monitor the behaviour of EU residents.

If your company processes the personal data of EU residents, whether directly or indirectly, you should be aware of the new rules and how they may affect your data processing and security systems and protocols, as well as the potential penalties for non-compliance.

Key Terms and Concepts

The GDPR uses the following terms and concepts:

"Personal data" is broadly defined as any information related to a living individual that could be used to directly or indirectly identify him or her. This includes name, photo, email address, bank details, medical information, computer IP address, cookie identifiers, and social media posts. "Sensitive Personal Data" is any information that reveals a person's racial or ethnic origin, political opinions, religious beliefs, health or sexual orientation, trade union membership, or genetic or biometric data. Such data is subject to additional protections.

"Controller" is any entity that determines, either alone or jointly with others, the purposes and means of the processing of personal data (whether that processing is automated or not). Essentially this is the organization, whether corporation, bank, hospital, *etc.,* that decides what personal data is collected and how, even if it does not directly collect the data itself.

LETTE is an established international law group with offices in Toronto, Montréal, Paris and Munich, offering a wide range of legal services to the business community. Whether acting for a multinational corporate group or for dynamic entrepreneurs, LETTE provides practical and effective solutions to its clients.

"Processor" is the entity that processes the personal data on behalf of a controller, such as a data center, document management company, cloud provider, or payroll service provider. An entity can be both a controller and processor if it processes personal data both for itself and for third parties.

"Data Minimization" is a key principle of the GDPR which requires that organizations only collect and process the minimum amount of personal data necessary for their specified purpose. Related to this concept are other data protection principles which organizations must bear in mind when considering their data processing activities:

- data processing should be fair, lawful, and transparent;
- data collected for one purpose cannot be use for a different purpose without further consent;
- data must be processed in a manner that ensures its security; and
- data should not be kept for longer than is necessary to achieve the purpose behind its processing.

As controllers will be held accountable for their organization's compliance with the GDPR's data protection principles, an understanding of these principles is crucial to an organization's ability to review and revise its data processing activities in accordance with the GDPR requirements.

Individual Privacy Rights

The enhanced privacy rights enjoyed by EU residents under the GDPR include:

- a right to access the personal data an organization has about them, including obtaining a copy of their data and information on how their data is processed, on what legal basis and for what purpose, for how long, and with whom it is shared;
- a right to object to the processing of their personal data in certain circumstances (such as for direct marketing purposes) and to restrict its processing (including automated decision-making);

- a right to be forgotten (*i.e.* a right to ask a data controller to delete their personal data in certain circumstances);
- a right to have their personal data transferred from one data controller to another;
- a right to have third parties notified of any rectifications to their personal data; and
- a right to receive clear and understandable information from data controllers about the scope and purpose of their data processing.

The GDPR imposes a legal obligation on controllers to give effect to the above rights of individuals. Organizations must thus ensure that they have systems in place to be able to adequately respond to data requests from individuals.

Data Protection Obligations

Some of the obligations on controllers and processors that stem from the above principles and rights are:

- Consent: Under the GDPR, organizations must be able to prove that they have a lawful ground for processing data. In most cases, that lawful ground will stem from a contract or from an individual's consent (other lawful grounds include the "legitimate interests" of a controller, the public interest, and compliance with legal obligations). A request for consent must be set out in plain language, include the purpose for which the personal data is required as well as the legal basis for processing, and be distinguishable from other matters when set out in a controller's written agreement or declaration. The consent given must be a "freely given, specific, informed and unambiguous" statement or clear affirmative action. An approach based on acquiescence, for example, in the form of pre-ticked boxes, will not constitute valid consent. Prior to consent being given, the individual must be advised of his/her right to withdraw consent, which must also be easily achievable. It is up to a controller to demonstrate that consent was properly obtained. Existing consents can only be relied upon if they meet the GDPR requirements.

- Data Security: Controllers and processors must implement appropriate technical and organizational security measures to protect personal data against accidental or unlawful destruction, loss, alteration, or unauthorised disclosure or access. These can include encryption, back-up facilities, and regular security reviews and testing.

- Breach: A controller must provide notification to the applicable supervisory authority (known as a national data protection authority or DPA, created by each EU member state to implement and enforce the GDPR) within 72 hours of becoming aware of a breach, unless the data breach is unlikely to result in any harm to the data subjects. A controller must also notify data subjects of a breach if there is a high risk to their rights and freedoms, subject to certain exceptions (such as if the data is rendered unintelligible to unauthorized persons through encryption or other means). A processor must notify the controller of a data breach without undue delay.

- Appointment of Processors: A controller may only use processors who guarantee compliance with the GDPR. The appointment must be in a written agreement which must impose certain mandatory obligations on the processor, including regarding confidentiality and data security, appointment of sub-processors, and assistance to controllers on various matters. In particular, a processor must follow a controller's documented instructions, but in the event of a perceived conflict between those instructions and GDPR or other EU or member state legal requirements, the processor must immediately inform the controller that it cannot comply with the latter's instructions.

- Data Protection Officers: Controllers and processors whose core activities consist of processing operations that require regular and systematic monitoring of individuals or who process certain categories of personal data (including Sensitive Personal Data) on a large scale must appoint a data protection officer, who must have expert knowledge of data protection laws and practices. As well, where a new processing activity may result in a high risk to individuals, a controller must first do a "Data Protection Impact Assessment" before implementing the new activity. High risk activities include the use of new technology, systematic monitoring, and large scale processing of Sensitive Personal Data.

- Appointment of Representatives: Controllers and processors established outside of the EU must appoint a representative in one of the EU member states where the controller or processor offers goods or services or monitors the behaviour of individuals, unless the processing is occasional, does not involve large-scale processing of certain data, including Sensitive Personal Data, and is low risk taking into account the nature, context, scope and purpose of the processing.

- Privacy by Design and by Default: The GDPR entrenches these principles which state, respectively, that organizations must consider data protection principles throughout the design and development of goods and services that involve the collection of personal data, and that the default settings for any new processing activity are at the highest level of privacy.

- Record-Keeping: Controllers and processors must keep specific records of their data processing activities, which must be provided on request to the DPA. This obligation does not apply to organizations with fewer than 250 employees unless their processing is: (i) likely to result in a risk to individuals' rights and freedoms, (ii) not occasional, or (iii) includes special categories of data including Sensitive Personal Data.

- Cross-Border Data Transfers: Organizations (controllers and processors) are prohibited from transferring personal data to a recipient outside of the EU unless (i) the recipient is in a jurisdiction deemed to have an adequate level of data protection (Canada is currently considered an "Adequate Jurisdiction", for organizations subject to PIPEDA, the federal privacy legislation, pursuant to a decision under the previous EU Directive); (ii) the organization has implemented one or more safeguards listed in the GDPR, including "Binding Corporate Rules" for transfers within a corporate group that have been approved by the DPA and standard data protection clauses adopted by or codes of conduct approved by the European Commission; or (iii) an exemption applies if certain conditions are met (for example, the GDPR allows for transfers on the basis of explicit consent or contractual performance).

Liability

The controller is primarily responsible for ensuring that its processing activities are compliant with the requirements of the GDPR and can be held liable for the failure of its processor to comply with the GDPR. However, as noted above, the GDPR also imposes data protection requirements directly upon processors and those who fail to comply with the GDPR or the controller's instructions may also be subject to fines, penalties and compensation claims.

DPAs can impose various sanctions, including warnings and audits, and administrative fines; the decision to impose a fine will take into account factors such as the nature, gravity and duration of any non-compliance, any mitigating actions taken, the level of negligence, *etc*. **The maximum fine that can be imposed under the GDPR for non-compliance is 4% of an organization's annual global turnover or 20M€, whichever is greater.**

Conclusion

It is vital for any company whose data processing activities may fall within the purview of the GDPR to ensure they are compliant by the enforcement date. Given the onerous requirements imposed by the GDPR, extensive steps are needed to determine and implement compliance, including reviewing all personal data held by an organization, its consent procedures and privacy policies, its data security systems, its breach notification protocols, and its outsourcing agreements. Companies (even SMEs) that have yet to prepare an assessment and implement the necessary steps to ensure GDPR compliance are facing a significant challenge if they wish to be compliant by May 28, 2018.

Patrizia Banducci
Lette LLP
40 University Avenue, Suite 904
Toronto ON M5J 1T1
T: +1 416-971-4897
E: pbanducci@lette.ca

Taya Talukdar
Lette LLP
40 University Avenue, Suite 904
Toronto ON M5J 1T1
T: +1 416-971-4846
E: ttalukdar@lette.ca