The European Union General Data Protection Regulation

Introduction

What is the General Data Protection Regulation (GDPR)?

The GDPR is enacted by the European Union (EU) and has come into force on 25 May 2018. It helps protect EU citizens' personal data and provide enhanced rights around it.

Whom will it affect and how?

Organisations in Hong Kong, even without establishment in the EU, may need to comply with the GDPR when they process personal data of individuals in the EU in connection with:

1) The offering of (paid or for free) goods or services to individuals in the EU; or
2) The monitoring of the behaviour of individuals in the EU.

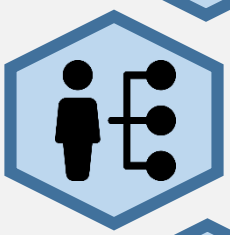
Sanctions if not compliant?

The maximum administrative penalty is a fine up to 20 million euros or 4% worldwide annual turnover, whichever is higher.

Highlights

Extra-territorial Application: The GDPR applies to processing activities involving personal data engaged by organisations/businesses established in non-EU jurisdictions, including Hong Kong.

Definition of "Personal Data": The definition of "Personal Data" is extended to include any information relating to an identified or identifiable natural person, e.g., name, address, identification number, location data, online identifiers such as cookies and IP addresses, sound and video recordings, still images, etc.



Special Categories of Personal Data: The "special categories" of personal data refer to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or data concerning a natural person's sex life or sexual orientation, and genetic data or biometric data processed for the purpose of uniquely identifying a natural person.

Transparency and Consent: The GDPR requires data controllers to provide extensive information to data subjects about the processing of their personal data in clear and plain language. Data subjects shall be presented with genuine and granular choice to give separate consents for different processing activities in form of unambiguous notice or clear affirmative action.

Enhanced Rights for Individuals: The GDPR enhances the rights of individuals in various aspects. Data subjects have the right to notice on data processing, rights to access, rectification or erasure of their data, rights to restriction or objection to processing, right to data portability, and right to not being subject to a decision based on automated processing, including profiling.

Data Breaches and Responses: The GDPR requires data controllers to notify and advise the supervisory authority in the EU member states of a data breach without undue delay (and where feasible, no later than 72 hours after becoming aware of it). If the breach is likely to result in a high risk to the rights and freedoms of individuals, the affected individuals must be notified without undue delay.

Privacy by Design and by Default: The GDPR requires data controllers to implement appropriate technical and organisational measures (such as pseudonymisation and data minimisation) which are designed to give effect to the data protection principles at the time of determining the processing activities, and to integrate the necessary safeguards with the processing.

Getting Prepared

Organisations/businesses are required to (i) demonstrate their compliance with the principles of processing of personal data[1]; (ii) implement appropriate technical and organisational measures to ensure compliance[2]; and (iii) integrate data protection into their processing activities[3]. More specifically, the following measures should be implemented or integrated into data protection processes:

- Appointment of a Data Protection Officer[4] (DPO) to monitor, implement and advise on compliance with the GDPR;
- Undertaking Data Protection Impact Assessment (DPIA) to identify and manage data protection risks;
- Undertaking Privacy by Design and by Default to give effect to the data protection principles at the time of determining the means of processing and to integrate the necessary safeguards;
- Keeping records of processing activities; and
- Drawing up data processing or handling policies or practices to demonstrate compliance and accountability.

*Note 1, 2, 3: referring to Article 5(2), Article 24 and Article 25 of the GDPR respectively.
Note 4: If processing personal data is not a core part of the business and the activity does not create risks for individuals, some obligations of the GDPR will not apply, e.g., appointment of a DPO.

Examples

When the GDPR is applicable

Your organisation is a small, tertiary education organisation operating online with an establishment based outside the EU. It targets mainly Spanish and Portuguese language universities in the EU. It offers free advice on a number of university courses and students require a username and a password to access your online materials. Your organisation provides the said username and password once students fill out an enrolment form. In this case, the GDPR is applicable.

When the GDPR is not applicable

Your organisation is a service provider based outside the EU. It provides services to customers outside the EU. Customers can use your services when they travel to other countries, including those within the EU. Provided that your organisation does not specifically target your services at individuals in the EU, the GDPR is not applicable.

Further Reading

EU GDPR	*https://ec.europa.eu/info/law/law-topic/data-protection_en*
UK ICO	*https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/*
HK PCPD	*https://www.pcpd.org.hk/english/data_privacy_law/eu/eu.html*