General Data Protection Regulation GDPR and PDPO

2021

Prof. Albert So
蘇文傑律師 / 客席法學教授

倫敦大學、劍橋大學、哈佛大學、牛津大學研究文憑
香港中文大學(醫學院)、香港大學客席講師
法律專欄作家
香港調解仲裁中心主席
執業律師，律政司(外聘)主控官
香港人壽保險從業員協會榮譽法律顧問
認可調解員，認可家事調解員,仲裁員
YMCA學術及法律顧問
認可反洗黑錢專家，認可金融罪案專家
東華三院朗晴綜合家庭服務中心義務法律顧問
香港特別行政區傑出學生聯會榮譽顧問
認可反洗黑錢專家，認可金融罪案專家
仁濟醫院/無國界醫生/保良局/匡智會/東華三院榮譽法律顧問
2018年度最傑出信託律師獎

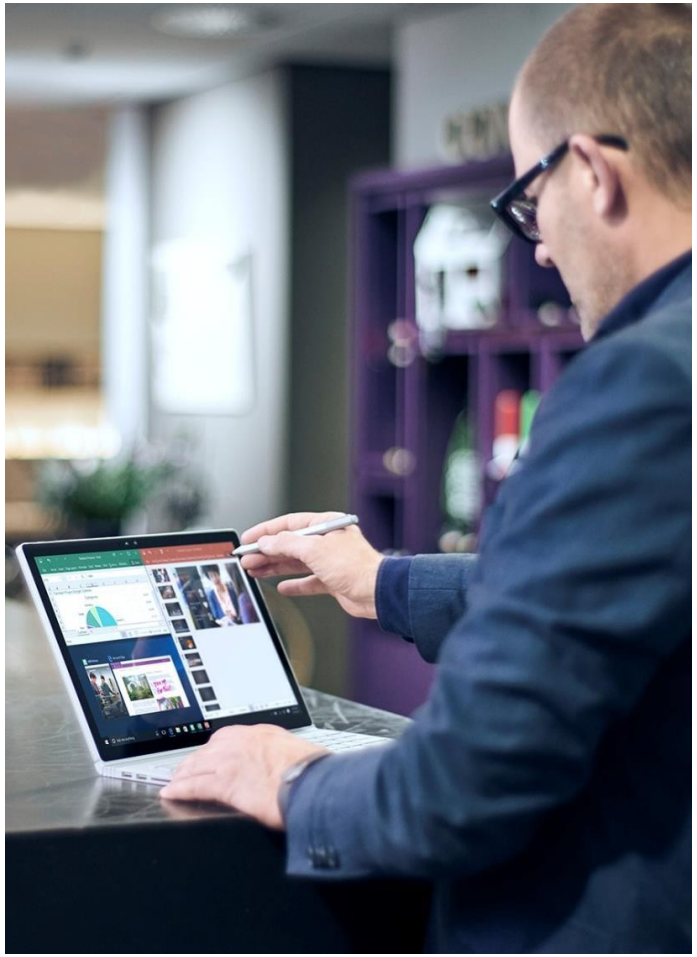
GDPR Topics

- What is the GDPR?
- How to interpret the GDPR
- GDPR Compliance Checklist
- Differences between GDPR and PDPO

GDPR key roles that will impact you

Controller (from GDPR)

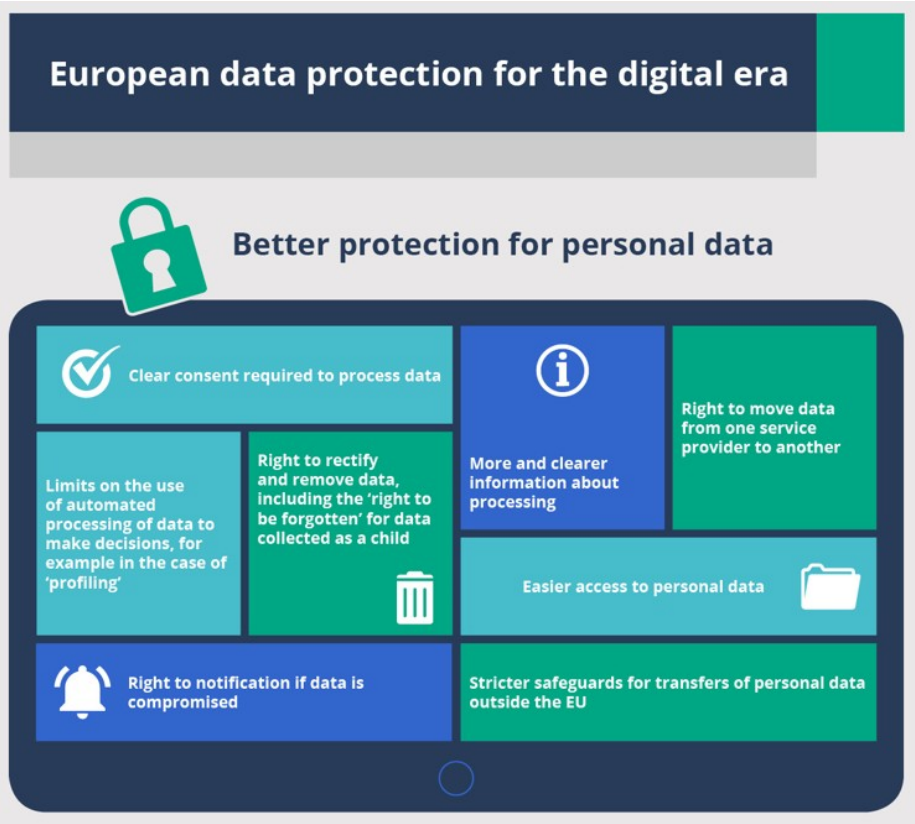
"…the natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing of personal data**; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."



Processer (from GDPR)

"…a natural or legal person, public authority, agency or other body which **processes personal data on behalf of the controller."**

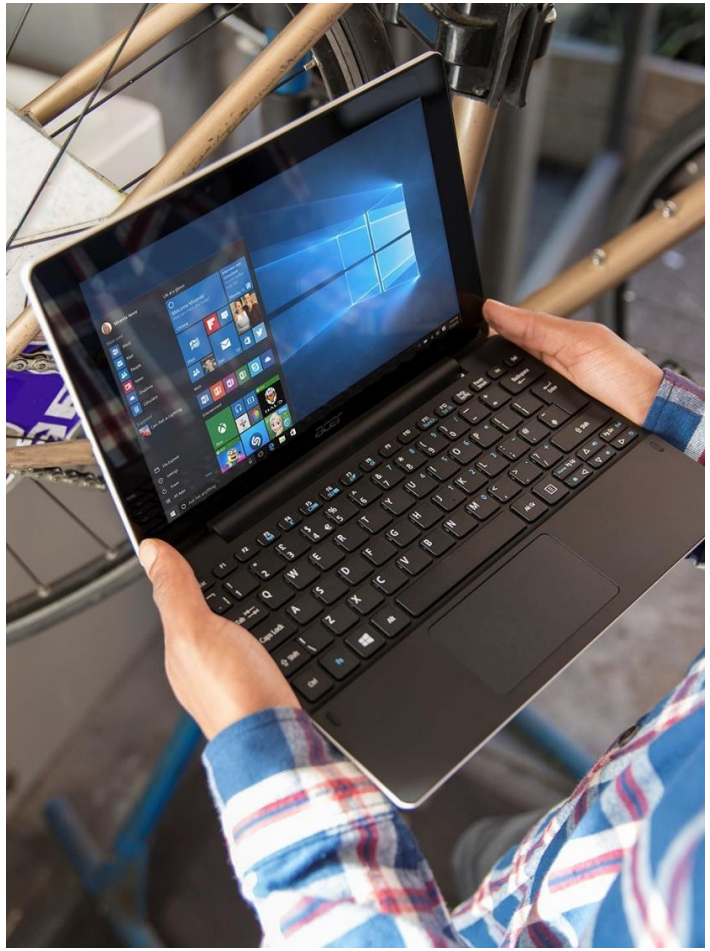
GDPR key drivers for May 25, 2018 enforcement



- Updates and modernizes the principles of the 1995 Data Protection Directive
- Sets out the rights of the individual and establishes the obligations of those processing and those responsible for the processing of the data.
- Establishes the methods for ensuring compliance as well as the scope of sanctions for those in breach of the rules.
- **Applies to all organizations doing business in the EU regardless of location.**

Source: European Council
Council of the European Union

GDPR data definitions regardless of nationality or EU residence



Personal Data (from GDPR)

"…means any information relating to an **identified or identifiable natural person ('data subject')**; an **identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier** such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Examples:

- Name
- Identification number (e.g., SSN)
- Location data (e.g., home address)
- Online identifier (e.g., e-mail address, screen names, IP address, device IDs)
- Genetic data (e.g., biological samples from an individual)
- Biometric data (e.g., fingerprints, facial recognition)

"The GDPR also **requires compliance from non-EU organizations that offer goods or services to EU residents or monitor the behavior of EU residents.**"

GDPR compliance is a challenge for both controllers and processors

"By the end of 2018, over 50% of companies affected by the GDPR will not be in full compliance with its requirements."

The General Data Protection Regulation (GDPR) imposes new rules on organizations that **offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents, no matter where they are located**.

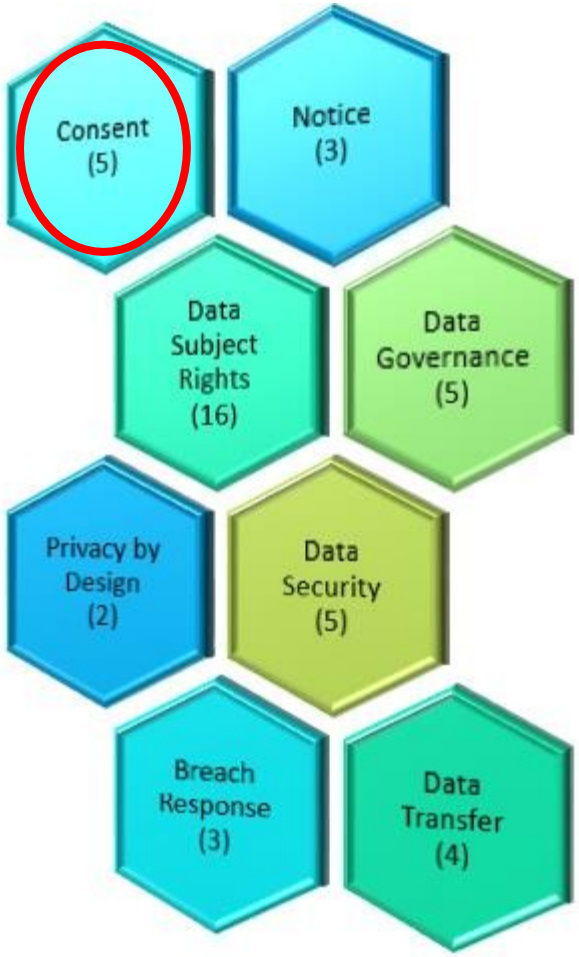
- **Enhanced** personal privacy rights
- **Increased** duty for protecting data
- **Mandatory** breach reporting
- **Significant** penalties for non-compliance

Controller's GDPR compliance

European Council
Council of the European Union

GDPR Regulation (261 pages)

43 GDPR Requirements*



1. Provide notification to data subjects, in **clear and plain language.**
2. Request and obtain the data subject's affirmative and granular **consent.**
3. Discontinue with processing activities if the data subject **denies consent**.
4. Provide a mechanism for data subjects to **withdraw consent**.
5. Obtain affirmative **consent from a child's (under age of 16) parent or guardian.**

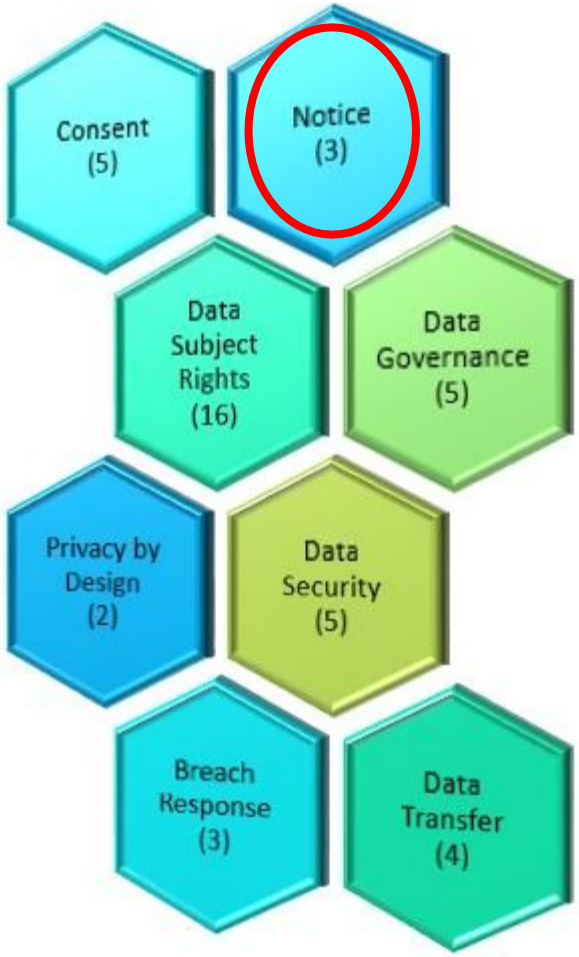
"…organizations must demonstrate that they have implemented appropriate measures to mitigate privacy risks. Even in the absence of a privacy breach or customer complaint, regulators may require firms to exhibit evidence of their compliance and risk management strategies, including a **privacy impact assessment (PIA)** when appropriate."

Controller's GDPR compliance

European Council
Council of the European Union

GDPR Regulation (261 pages)

43 GDPR Requirements*



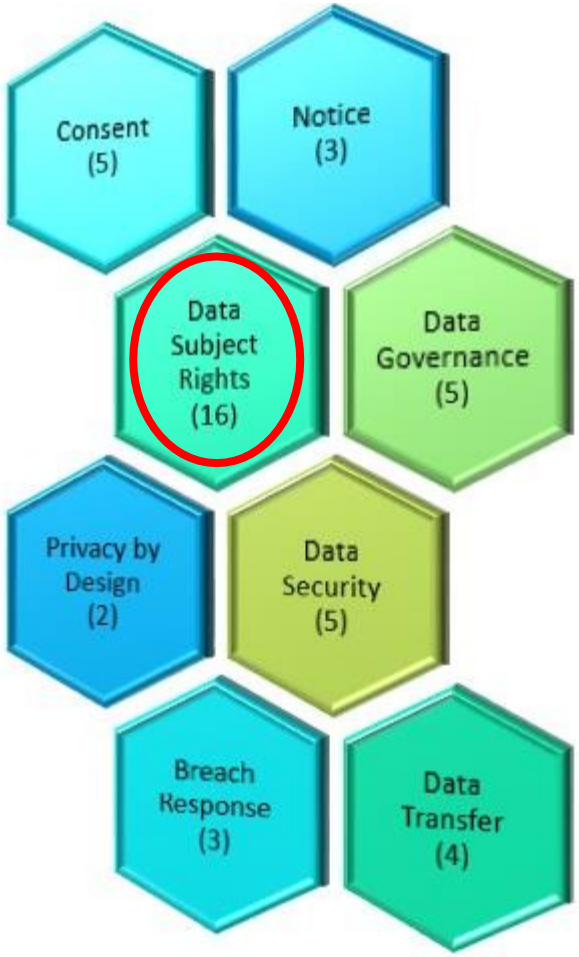
1. Provide **notice of processing activities** at the time personal data is **obtained**.
2. Provide notice of processing activities if personal data has not been obtained directly.
3. Provide the data privacy notice at **all points** where **personal data is collected**.

Controller's GDPR compliance

European Council
Council of the European Union

GDPR Regulation (261 pages)

43 GDPR Requirements*



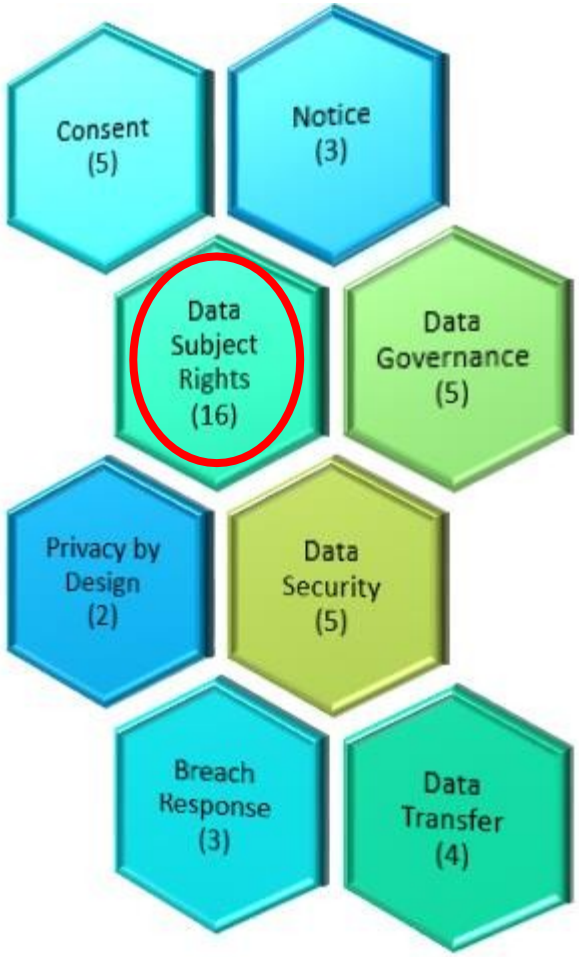
1. Provide mechanism for validating identity of the requesting data subject.
2. Provide mechanism for to **request access to their personal data.**
3. Provide a mechanism to **respond to requests** on personal data access.
4. Maintain the technological ability to **trace and search personal data.**
5. Provide mechanism to **request rectification** and rectify personal data.
6. Provide a mechanism to request the **erasure of personal data.**
7. Maintain the technological ability to **locate and erase personal data.**
8. Track to which **additional controllers** personal data has been **transferred**.

Controller's GDPR compliance

European Council
Council of the European Union

GDPR Regulation (261 pages)

43 GDPR Requirements*



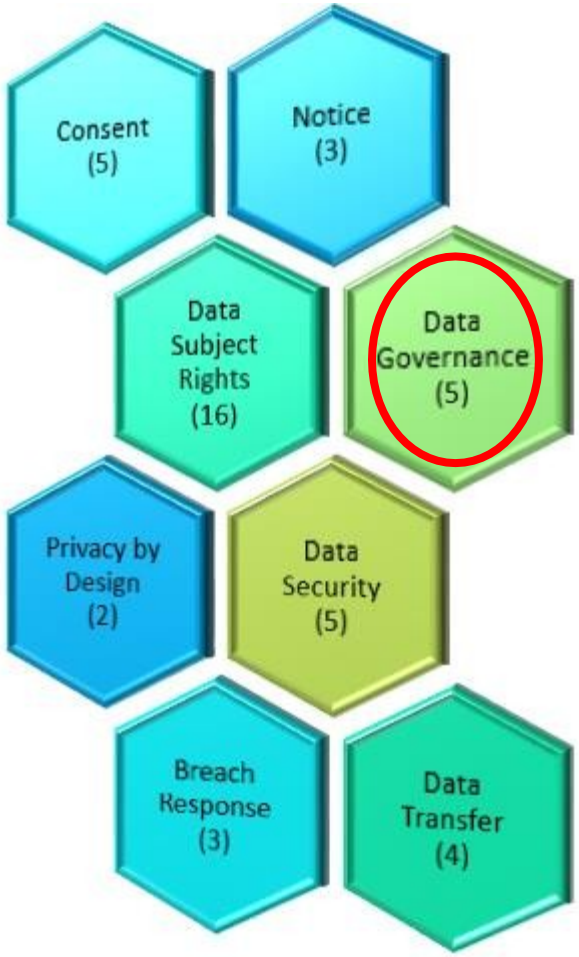
9. When personal data is made public, contact those entities for **data erasure**.
10. Provide mechanism to request the **restriction of data processing.**
11. Maintain the technological ability to restrict processing of personal data.
12. Provide mechanism to **request copies and transmit personal.**
13. Provide mechanism to respond to **data portability requests.**
14. Locate personal data and **export in structured, machine-readable formats**.
15. If processing for **direct marketing**, provide mechanism to **object**.
16. Maintain the technological ability to discontinue the data processing.

Controller's GDPR compliance

European Council
Council of the European Union

GDPR Regulation (261 pages)

43 GDPR Requirements*



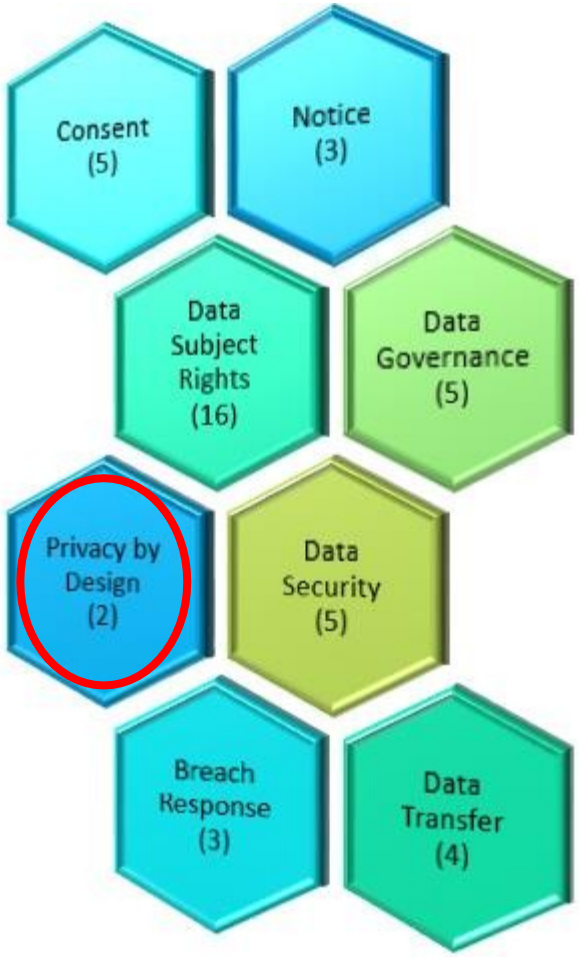
1. **Maintain audit trails** to demonstrate accountability and compliance.
2. Maintain **inventory** of data detailing categories of data subjects.
3. Maintain **auditable trails** of processing activities.
4. Carry out **data protection impact assessments (DPIA)** of processing operations.
5. Provide the de-identification of personal data for **archiving purposes**.

Controller's GDPR compliance

European Council
Council of the European Union

GDPR Regulation (261 pages)

43 GDPR Requirements*



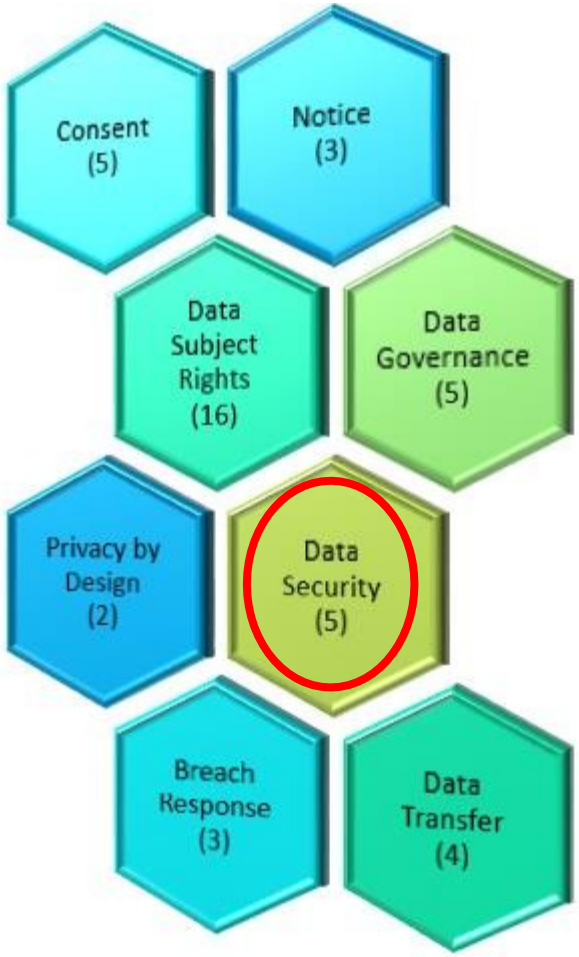
1. Embed privacy controls.
2. Embed **privacy design** to minimize the amount of personal data collected.

Controller's GDPR compliance

European Council
Council of the European Union

GDPR Regulation (261 pages)

43 GDPR Requirements*



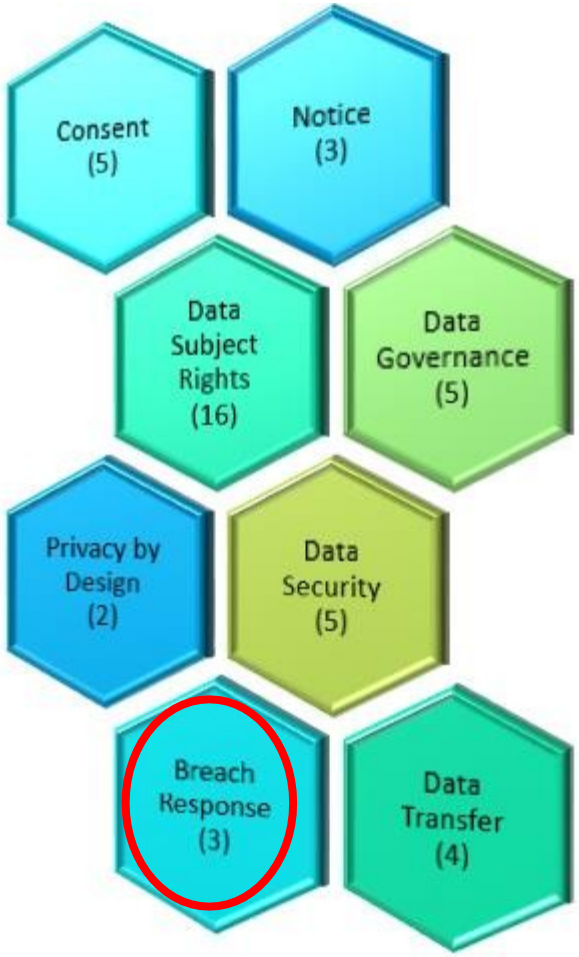
1. Provide mechanism to **pseudonymize, encrypt**, or otherwise secure personal data.
2. Implement **security measures** in the service.
3. Confirm ongoing confidentiality, integrity, and availability of personal data.
4. Provide mechanism to restore the availability and access to personal data.
5. Facilitate regular testing of security measures.

Controller's GDPR compliance

European Council
Council of the European Union

GDPR Regulation (261 pages)

43 GDPR Requirements*



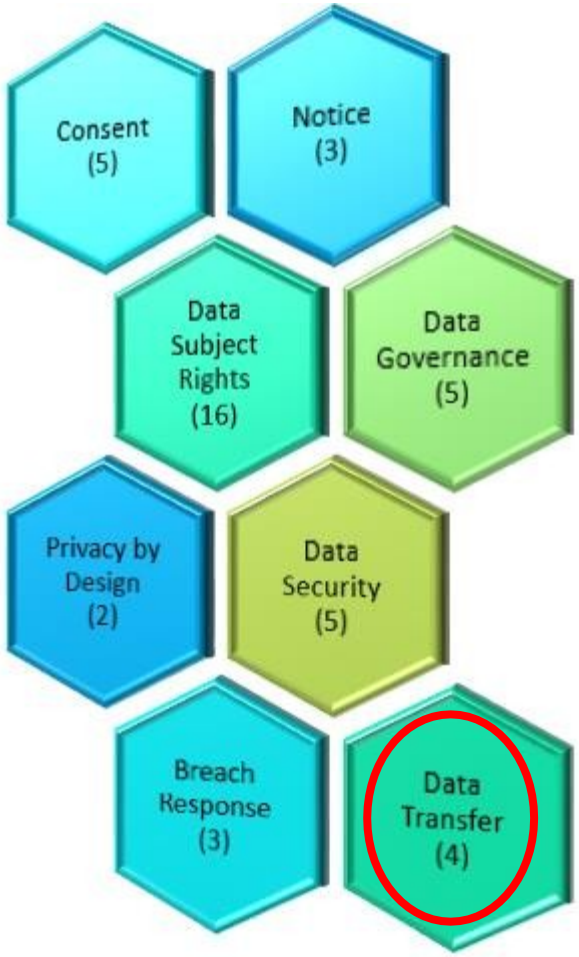
1. Controllers **notify Data Protection Authority within 72 hours** in the event of a data breach incident.
2. Controllers **notify affected data subjects** of a high-risk data breach incident.
3. Processors notify controllers without undue delay of a data breach incident.

Controller's GDPR compliance

European Council
Council of the European Union

GDPR Regulation (261 pages)

43 GDPR Requirements*



1. **Track and record** personal data that is forwarded to **third-parties**.
2. Provide mechanism for tracking and recording data transfers **in and out of the EU**.
3. Maintain inventory of data transfer contracts with third-parties.
4. Provide appropriate safeguards (e.g., Privacy Shield) for effective legal remedies.

Difference between GDPR and PDPO?

PDPO – GDPR Comparative Study

PCPD identified the following 9 major differences between PDPO and GDPR:

9 Major Differences	
1. Extra-Territorial Application	6. Data Processor Obligations
2. Accountability and Governance	7. New or Enhanced Rights of Data Subjects/Profiling
3. Mandatory Breach Notification	8. Certification/Seals and Personal Data Transferred Outside Jurisdictions
4. Sensitive Personal Data	9. Sanctions
5. Consent	

1. Extra-Territorial Application

EU GDPR	HK PDPO
Data processors or controllers: • with an establishment in the EU, or • established outside the EU, that offer goods or services to individuals in the EU, or monitor the behaviour of individuals in the EU. [Art 3]	**Data users** who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the personal data in or from Hong Kong. [S.2(1)]

2. Accountability and Governance

EU GDPR	HK PDPO
Risk-based approach to accountability. Data controllers are required to: • implement technical and organisational measures to ensure compliance [Art 24]; • adopt data protection by design and by default [Art 25]; • conduct data protection impact assessment for high-risk processing [Art 35]; and • (for certain types of organisations) designate Data Protection Officers [Art 37].	The accountability principle and the related privacy management tools are not explicitly stated. The Privacy Commissioner advocates the Privacy Management Programme which manifests the accountability principle. The appointment of data protection officers and the conduct of privacy impact assessment are recommended good practices for achieving accountability.

3. Mandatory Breach Notification

EU GDPR	HK PDPO
• Data controllers are required to notify the authority about a data breach without undue delay (exceptions apply). • Data controllers are required to notify affected data subjects unless exempted. [Arts 33-34]	• No mandatory requirement. Voluntary breach notification.

4. Sensitive Personal Data

EU GDPR	HK PDPO
• Expand the category of sensitive personal data. • Processing of sensitive personal data is allowed only under specific circumstances. [Art 9]	• No distinction between sensitive and non-sensitive personal data.

5. Consent

EU GDPR	HK PDPO
• One of the 6 lawful bases for processing • Consent must be ✓ freely given, specific and informed; and ✓ an unambiguous indication of a data subject's wishes, by statement or by clear affirmative action, which signifies agreement to the processing of his personal data. [Art 4(1)]	Consent is not a pre-requisite for the collection of personal data, unless the personal data is used for a new purpose. [DPPs 1&3] 

6. Data Processor Obligations

EU GDPR	HK PDPO
• Data processors are imposed with additional obligations, such as: maintaining records of processing, ensuring security of processing, reporting data breaches, designating Data Protection Officers, etc. [Arts 30, 32-33, 37]	• Data processors are not directly regulated. • Data users are required to adopt contractual or other means to ensure data processors comply with data retention and security requirements. [DPPs 2&4]

7. New or Enhanced Rights of Data Subjects / Profiling

EU GDPR	HK PDPO
• Right to erasure of personal data (also known as "right to be forgotten") [Art 17] • Right to data portability [Art 20] • Right to object to processing (including profiling) [Art 21] • "Profiling" is defined as any form of automated processing involving personal data to evaluate certain personal aspects of a natural person [Art 4(4)] • Expanded notice requirement for the new or enhanced rights	• No general right to erasure, but shall not retain personal data for longer than necessary [S.26 & DPP 2(2)] • No right to data portability • No general right to object to processing (including profiling), but may opt out from direct marketing activities [Ss.35G &35L] and contains provisions regulating data matching procedure [Ss. 30-31]

8. Certification / Seals and Personal Data Transferred Outside Jurisdictions

EU GDPR	HK PDPO
• Explicitly recognises privacy seals and establishes certification mechanism for demonstrating compliance by data controllers and processors. [Art 42] • Certification as one of the legal bases for cross-border data transfer.	• No such certification or privacy seals mechanism for demonstrating compliance.

9. Sanctions

EU GDPR	HK PDPO
• Data protection authorities can impose administrative fines on data controllers and processors. [Art 58]	• The Privacy Commissioner is not empowered to impose administrative fines or penalties.
• Depending on the nature of the breach, the fine could be up to €20million or 4% of the total worldwide annual turnover. [Art 83]	• The Privacy Commissioner may serve enforcement notices on data users.

General Data Protection Regulation GDPR and PDPO

「法律迷思」蘇文傑

蘇文傑律師
Albert So

Live WhatsApp
法律熱線 9825 2500

如有任何相關法律問題

法律專欄文章

請到以下連結留言

「法律迷思」蘇文傑

蘇文傑律師
Albert So

如有任何財富承傳相關法律問題

albertso@trust-wealth.org

法律專欄文章

請到以下連結留言

TRUST
WEALTH SUCCESSION PLANNING ASSOCIATION
財富承傳策劃協會

Live WhatsApp
法律熱線 9825 2500