



GDPR VS THE WORLD

PART 1 GDPR VS ASIA

Hong Kong 

China

India

Indonesia

Japan

Malaysia

Singapore

South Korea

Thailand

UAE



**How much has the GDPR driven
data protection worldwide ?**

**An in-depth comparison of different legislations
around the world based on 35 criteria**

Authors



Adam Ali-Bey

IT Legal Expert and Main Author



Sumedha Ganjoo

Legal Research Lead



Katia Bouslimani

Chief Legal Research Officer



Stéphanie Exposito-Rosso

IT Legal Expert



Antoine Piquet

IT Legal Expert



Eloïse Quinzin

IT Legal Expert and Main Author

We would like to thank Bianca Kunrath, Era Selmani and Ylli Kodza for their feedback.

The information provided in this publication is general and may not apply in a specific situation. The publishers and authors accept no responsibility for any acts, errors or omissions contained herein. The information provided was verified between October 2021 and October 2022. Note that the regulation is meant to evolve.

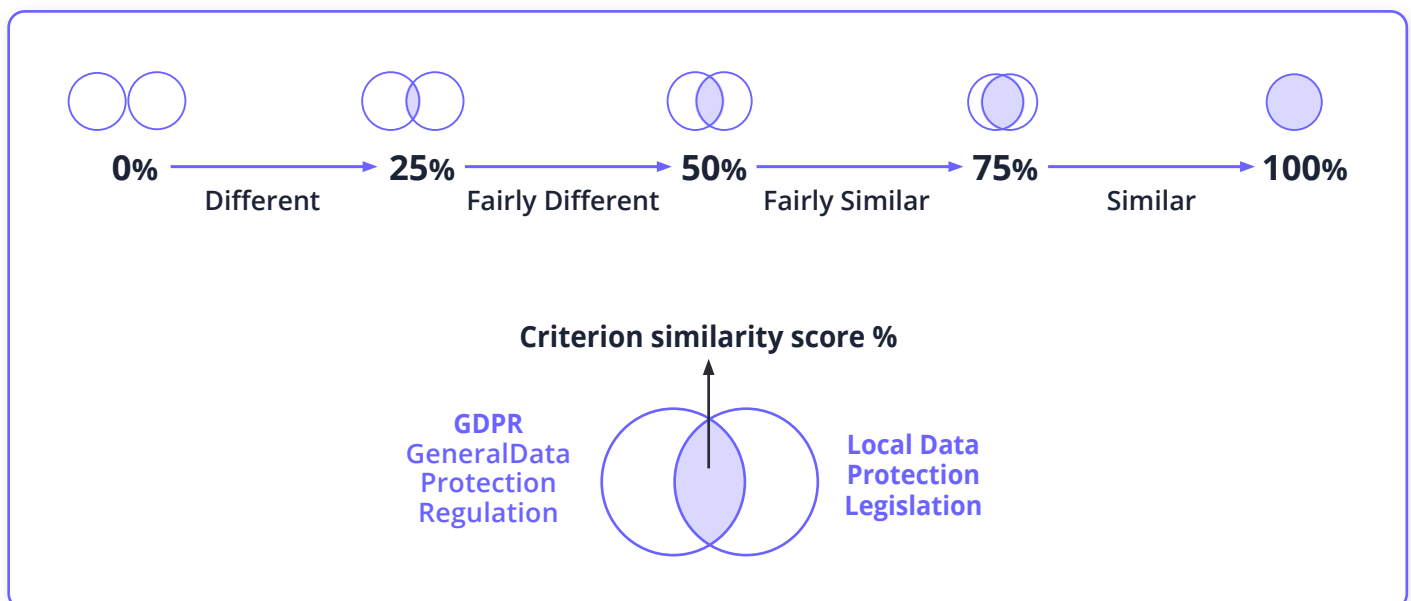
Published September 2022

Welcome to the “GDPR VS” Series

The General Data Protection Regulation (GDPR) was adopted in 2016 by the European Parliament and the European Council, and entered into force on 25 May 2018. Innovative by its extensive scope, provisions and enforcement potential, the GDPR made a lot of noise and required companies to provide efforts of compliance.

25 May 2022 is the fourth anniversary of the GDPR, and a pertinent time to ask: Has the GDPR created “a recipe for the world?” [Code is Law \(Alias.dev\)](#) aims to assess the level of influence of the GDPR in different regions of the world that have adopted or have not adopted new data protection regulations since 2016. The objective is to help companies conduct their gap analysis between different data protection legislations in their data protection compliance efforts.

[Alias.dev](#) chose 35 criteria to compare the GDPR with other data protection legislation, and analysed these criteria through more than 200 sub-criteria. Each criterion is given a similarity score. The score indicates how much effort GDPR-compliant companies will have to engage to comply with data protection legislation outside the EU and understand the data protection culture of the jurisdiction. The similarity score is as follows:



Contents

05 List of Acronyms

06 Introduction

07 Scope

Criterion 1. The Territorial Scope /7

Criterion 2. The Subject Matter Scope /8

Criterion 3. Definition of Personal Data /9

Criterion 4. Definition of Sensitive Personal Data /10

Criterion 5. Relevant Parties /11

13 Lawfulness

Criterion 6. Legal Bases /13

Criterion 7. Consent /14

Criterion 8. Legitimate Interest /15

Criterion 9. Conditions for Processing of Sensitive Data /16

Criterion 10. Children /18

19 Data Subjects' Rights

Criterion 11. Transparency Requirements /19

Criterion 12. Right of Access /20

Criterion 13. Right to Data Portability /21

Criterion 14. Right to Rectification /21

Criterion 15. Right to be Forgotten / Right to erasure /22

Criterion 16. Right to Object /23

Criterion 17. Rights Related to Profiling /24

Criterion 18. Right to Restrict the Use of the Personal Data /24

25 Accountability Requirements

Criterion 19. Appointment of a Representative /25

Criterion 20. Appointment of a DPO /25

Criterion 21. Record of processing /26

Criterion 22. Data Protection Impact Assessment (DPIA) /27

Criterion 23. Privacy by Design / Right to Erasure /28

Criterion 24. Audit Requirements /28

Criterion 25. Appointment of Processors /29

Criterion 26. Information Security /30

Criterion 27. Breach Notification /31

32 Data Localisation and Transfer

Criterion 28. Data Localisation Requirements /32

Criterion 29. International Data Transfer /32

34 Enforcement

Criterion 30. Data Protection Authority /34

Criterion 31. Penalties /35

36 Exemptions

Criterion 32. Anonymised Data /36

Criterion 33. Social Media Intermediaries and Identity Managements /36

Criterion 34. Exemptions for Research /37

Criterion 35. Application to Public Authorities /38

39 Conclusion

40 Compliance-as-Code: Our Solution

List of Acronyms

A

AAB: Administrative Appeals Board

C

CSJ: Chartered Secretary

D

DDP: Data Protection Principle

DPIA: Data Protection Impact Assessment

DPO: Data Protection Officer

G

GDPR: General Data Protection Regulation

I

ICT: Information and Communication Technology

P

PCPD: Privacy Commissioner for Personal Data

PD(P)O: Personal Data (Privacy) Ordinance

PIPL: Personal Information Protection Law (China)

PMP: Privacy Management Programme

Introduction

The Personal Data (Privacy) Ordinance (Cap. 486), the PD(P)O, governs the acquisition and management of personal data.

There are six Data Protection Principles (DPPs) that are the core of the Ordinance and cover the life cycle of data. These are set out in Schedule 1 to the PD(P)O. The DPPs describe how Data Users should collect, handle and use the personal data of Data Subjects. The DPPs are:

1. Purpose and Manner of Collection of Personal Data
2. Accuracy and Duration of Retention of Personal Data
3. Use of Personal Data
4. Security of Personal Data
5. Information to be Generally Available
6. Access to Personal Data

The Ordinance has been in effect since 1996, but was considerably revised in 2012/2013, notably with regard to direct marketing. Most recently, in October 2021, the Personal Data (Privacy) (Amendment) Ordinance, the “Amendment Ordinance”, came into effect, introducing additional doxxing offences and associated punishments.

The Amendment Ordinance initially contained a number of other recommended changes to the PD(P)O. These are outlined in the January 2020 consultation paper (LC Paper No. CB(2)512/19-20(03)). The additional amendments are currently being evaluated by the Legislative Council, and there is no indication of when they will be enacted.

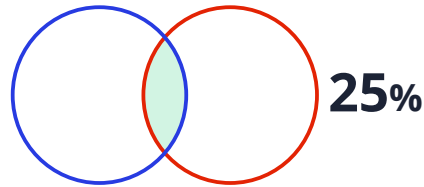
The Data Protection Authority is called the Office of the Privacy Commissioner for Personal Data (PCPD) and is responsible for monitoring, supervising, promoting, and enforcing the provisions of the Personal Data (Privacy) Ordinance (PD(P)O). The PCPD is an independent body established on 1 August 1996. Currently, the chairman is Ms Ada CHUNG Lai-ling.

The PCPD is divided into different functional divisions: the Administration Division, Finance Division, Legal Division, Operations Divisions, Compliance & Policy Division, Information Technology Division, and the Corporate Communications Informations Division.

The PCPD has an important role in respect of privacy in Hong Kong. In addition to being able to sanction those who do not respect the laws on the matter, it often issues non-binding guidelines to explain the rights of individuals and their application.

Scope

Criterion 1. The Territorial Scope



Fairly Different



Article 3

The GDPR is applicable when there is the presence of an “establishment” in the EU, which means that the Data Controller or the Data Processor exercises an effective and real activity (even a minimal one) through stable arrangements.

Extraterritorial scope: applies when a Data Controller or a Data Processor that is located outside the EU processes activities that are related to the offering of goods or services (regardless of the existence of a payment) to Data Subjects in the EU or to the monitoring of their behaviour as far as their behaviour takes place within the EU.

Case No.2019A07, AAB Appeal No.15 of 2019

PD(P)O

The PD(P)O is silent about its territorial application.

The PD(P)O has no extraterritorial effect.

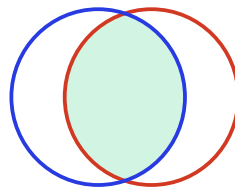
“The Administrative Appeals Board (AAB) agreed with the Commissioner’s interpretation that the Ordinance did not have any extra-territorial effect.” (Case No.2019A07, AAB Appeal No.15 of 2019)

A decision on 7 August 2020, reiterated this principle.

Contrary to the GDPR, which requires an establishment in the European Union to meet the territorial criterion, the PD(P)O is silent about its territorial application. However, the Administrative Appeals Board stated that the PD(P)O had no extraterritorial effect, contrary to the GDPR, which explicitly applies outside the EU.

Scope

Criterion 2. The Subject Matter Scope



70%

Fairly Similar



Article 1

The GDPR's aims are clearly defined: to protect the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data and to protect and encourage the free movement of personal data within the EU.

If the data is part of a file system, the GDPR applies to the processing of personal data by automated or non-automated methods.

The GDPR does not apply to anonymised data.

The GDPR exempts:

- Personal data processed by people for solely personal or domestic reasons that has "no relation to a professional or commercial activity".
- Data processed in the context of law enforcement or national security.

The GDPR establishes standards for some types of processing, such as processing for journalistic purposes and processing for academic, artistic, or literary expression.

Part 1. Preliminary (2), Part 8. Chartered Secretaries (CSJ), Privacy Compliance – A Marathon not a Sprint¹

PD(P)O 

The PD(P)O explicitly provides that it aims to protect the privacy of individuals. However, in 2018 the PDPC stated that the PD(P)O "also facilitates economics and ICT development in Hong Kong".

The PD(P)O applies to personal data relating to living individuals, in a way that access to or processing of the data is practicable. The definition of personal data seems to exclude anonymised data from the PD(P)O's scope.

The PD(P)O exempts:

- Processing of personal data for domestic or recreational purposes.
- Processing of personal data by a court, a judge or a judicial officer in the course of performing judicial functions.
- Processing of personal data under an Interception of Communications and Surveillance Ordinance.

The PD(P)O also establishes specific derogations for some types of processing, including personal data related to employment, scholarships, personal reference, national security, law enforcement, health data in some circumstances, personal data related to a minor held by the Hong Kong Police Force or Customs and Excise Department, legal professional privilege, self-incrimination, legal proceedings, news, statistics, and research.

While the PD(P)O aims to protect individuals' personal data, the GDPR pursues the larger aim of protecting both fundamental rights and freedoms and the EU's single market.

The GDPR applies as long as personal data is part of a file system, while the PD(P)O requires the personal data's access or processing to be "practicable". Despite the different wording, both scopes overlap most of the time. Moreover, neither the PD(P)O nor the GDPR apply to anonymised data.

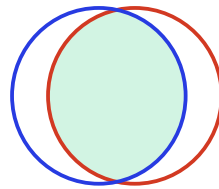
Both the GDPR and the PD(P)O exclude from their scope the processing of personal data for domestic or recreational purposes. While the GDPR exempts law enforcement and national security processing from its scope, the PD(P)O only provides partial exemptions for these purposes.

The GDPR establishes some derogations for some types of processing, such as processing for journalistic purposes and processing for academic, artistic, or literary expression. The PD(P)O also establishes some derogations but they are wider as they also encompass employment, some health data, legal proceedings, etc.

¹ Chadi Hantouche, "GDPR compliance: a marathon not a sprint" (2018), CGj, the monthly journal of The Hong Kong Chartered Governance Institute, <https://cgj.hkcgj.org.hk/2018/02/gdpr-compliance-a-marathon-not-a-sprint/>

Scope

Criterion 3. Definition of Personal Data



80%

Similar



Article 4, (1), (13), (14), (15),
Article 9

Personal data is defined by the GDPR as:

- Any information relating to an identified or identifiable natural person ("Data Subject").

An identifiable natural person, according to the GDPR, 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 one or more factors specific to that natural person's physical, physiological, genetic, mental, economic, cultural, or social identity.

Online identifiers, such as IP addresses, cookie identifiers, and radio frequency identifying tags, are considered personal data under the GDPR.

The GDPR does not apply to deceased people.

The GDPR does not apply to data that has been "anonymised" that can no longer be used to identify the Data Subject.

Section 6

PD(P)O 

Personal data is defined by the PD(P)O as "any data:

- (a) relating directly or indirectly to a living individual;
- (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
- (c) in a form in which access to or processing of the data is practicable."

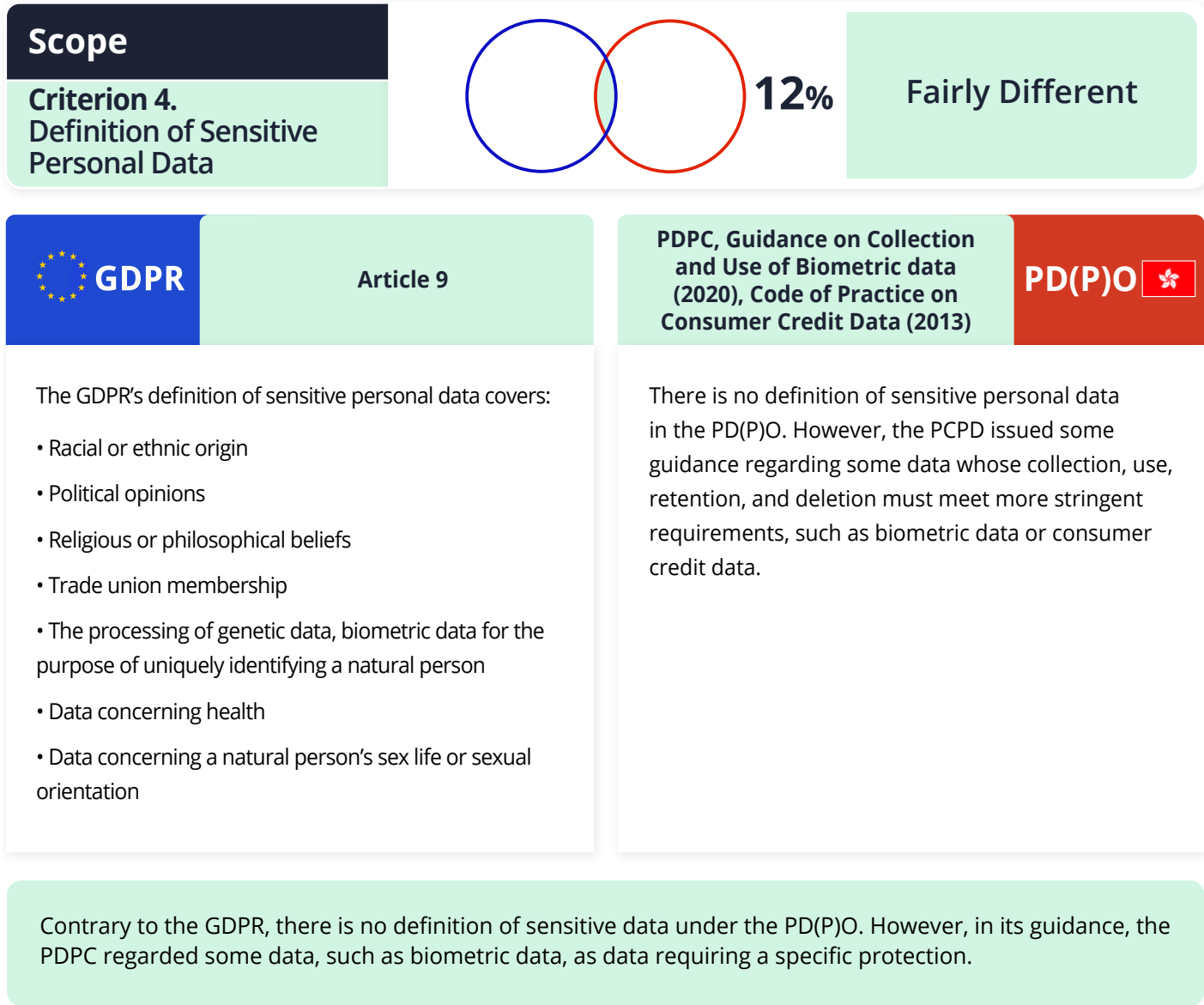
The PD(P)O does not apply to anonymised data.

Both the GDPR and the PD(P)O define personal data as data that can directly or indirectly identify an individual. Proposed amendments of the PD(P)O are considering explicitly referring to "identifiable" persons in the text of the PD(P)O.

Neither the GDPR nor the PD(P)O apply to anonymised data.

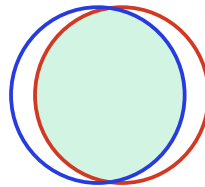
However, contrary to the GDPR, the PD(P)O includes in its definition data that is "in a form in which access to or processing of the data is practicable".

The PD(P)O explicitly excludes data related to deceased individuals from its definition of personal data. On the other hand, data related to deceased persons seems to be implicitly excluded from the GDPR.



Scope

Criterion 5. Relevant Parties



88%

Similar



Article 4 (7), 28, 30, 82

- A Data Controller is a natural or legal person, public authority agency, or other organisation that, alone or collectively with others, decides the goals and methods of processing personal data.

- A Data Processor is a natural or legal person, government agency, or other entity that processes personal data on behalf of the Data Controller.

Data Controllers must adhere to the purpose restriction and accuracy principles, and repair any inaccurate or incomplete personal data held by a Data Subject. They are required to put in place technological and organisational security measures, and alert supervisory authorities in the event of a data breach.

Data Controllers and Data Processors are required to retain records of processing operations, although small businesses are exempt from this need. Data Controllers and Data Processors can also designate a DPO.

Where processing is carried out on behalf of a Data Controller, the Data Controller must only use Data Processors who can provide sufficient guarantees to implement the appropriate technical and organisational measures to ensure that processing complies with the GDPR's requirements and protects the Data Subject's rights. Furthermore, without the Data Controller's previous explicit or general written authorisation, the Data Processor may not engage another Data Processor.

No examination system is named. However, the GDPR states that "time limits for erasure or periodic review should be established by the Data Controller".

In specific cases, the GDPR requires a Data Controller or Data Processor to complete a DPIA.

Part 1 – Preliminary (2),
Schedule 1, Principle 2(3),
Schedule 1, Principle 4(2)

PD(P)O

- A Data User is a person who, either alone or jointly with other persons, controls the collection, holding, processing or use of personal data.

- A Data Processor is a person who processes personal data on behalf of a Data User instead of their own purposes.

Data Users are required to comply with the PD(P)O, while Data Processors are not directly regulated under the PD(P)O.

Data Users are required to, by contractual or other means, ensure that their Data Processors meet the applicable requirements of the PD(P)O, including:

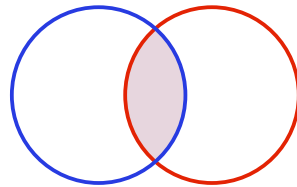
- Preventing any personal data transferred from being kept longer than necessary.
- Preventing unauthorised or accidental access, processing, erasure, loss or use of the personal data transferred.

Both the GDPR and the PD(P)O define the Data Controller (Data User in the PD(P)O) as the person who decides on the processing and the Data Processor as the person who processes personal data on behalf of the Data Controller (Data User in the PD(P)O). Moreover, both laws require Data Controllers to comply with the data protection principles they provide.

However, the GDPR and PD(P)O differ in the rules applicable to Data Processors. In the GDPR, Data Controllers are required to verify that the processor is able to comply with the data protection rules, but the Data Processor is still required to comply with the GDPR. In the PD(P)O, the Data User is required to ensure (by contract or otherwise) that the Data Processor complies with the PD(P)O, but the Data Processor is not directly subject to the PD(P)O.

Lawfulness

Criterion 6. Legal Bases



37%

Fairly Different



Articles 6-10 Recitals 39-48

Processing is lawful only if and to the extent that at least one of the following applies:

- The Data Subject has given consent to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of personal data, in particular where the Data Subject is a child.

Sections 35.A and 35.E, DPP 1,
Section 60.B, Part 8, Personal Data
(Privacy) Law in Hong Kong –
A Practical Guide on
Compliance (point 5.2)

PD(P)O 

The Data User may only process personal data if it is necessary and lawful for the processing they intend to do. However, the PD(P)O does not provide an exhaustive list of legal bases.

The consent of the Data Subject is sometimes required (for instance, matching procedures, use of personal data for new purposes, and in some cases of direct marketing).

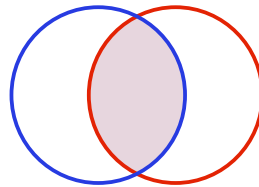
Some legal bases are indicated to be derogations to some provisions of the PD(P)O, such as employment, security, law enforcement, health, care and guardianship of minors, legal proceedings, news, statistics and research, etc.

These legal bases could indicate that the PD(P)O allows processing of data for the performance of a contract, for compliance with a legal obligation and for carrying out a task in the public interest. In general, the principle of lawfulness allows wide interpretation according to the Commissioner.

The GDPR and the PD(P)O both provide that processing of personal data must be lawful. However, the implementation of the principle of lawfulness differs. The GDPR provides an exhaustive list of legal bases on which Data Controllers can base their processing of personal data. The PD(P)O does not provide such a list and simply defines situations where consent is required and some legal bases for direct marketing purposes. The PD(P)O also provides situations in which it does not apply.

Lawfulness

Criterion 7. Consent



55%

Fairly Similar



Article 4(11), Article 7, Recital 32,
Recital 42, Recital 43

The GDPR establishes a set of criteria for gaining valid consent:

- Consent must be freely given, specific and informed.
- It must be granted by an unambiguous, affirmative action where the Data Subject signifies agreement to the processing of personal data relating to them.
- Generally, provision of a service cannot be made conditional on obtaining consent for processing that is not necessary for the service.
- A request for consent must be distinct from any other terms and conditions.
- The consent can be easily withdrawn at any moment "without prejudice".

Sections 35.A and 35.E

PD(P)O

The legal basis for consent is required when the Data User wishes to use the data for a different purpose than originally intended, and when the Data User wants to use the data for direct marketing purposes (except in some circumstances).

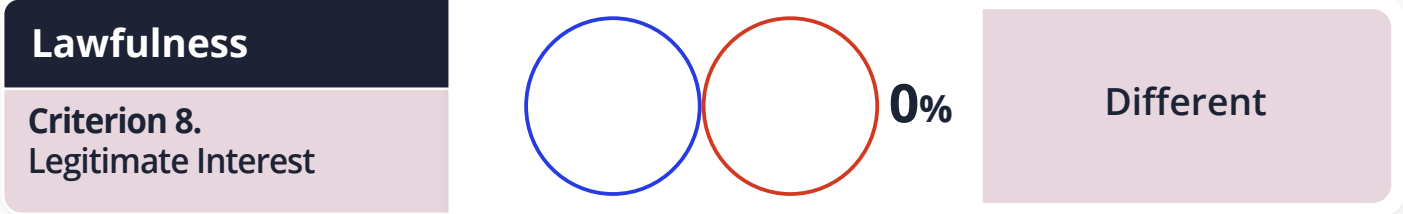
In the context of the marketing purpose, consent is defined as an indication of no objection to the use or provision. The consent must be informed, obtained in writing (when obtained orally, the Data User must send a written confirmation to the Data Subject), and that it is express and given voluntarily. Moreover, consent can be withdrawn by notice in writing.

Before using personal data in direct marketing, the Data User must provide the Data Subject with a channel through which the Data Subject may, without charge by the Data User, communicate the Data Subject's consent to the intended use.

The GDPR and the PD(P)O both provide that consent shall be informed and voluntarily given. The GDPR is, however, more specific than the PD(P)O as it insists on the fact that the information should be distinct from any terms and conditions and that free consent also means that it cannot be conditional on the provision of a service. The GDPR and the PD(P)O both provide that consent can be withdrawn by the Data Subject.

The PD(P)O provides that consent shall be obtained in writing (or be confirmed in writing). The GDPR does not provide such a requirement, but because consent shall be demonstrable, in practice, most of the consents will be given in writing. The PD(P)O provides that the consent shall be express, while the GDPR is more protective and provides that the consent should be provided by a statement or a clear affirmative action.

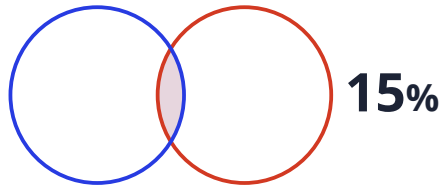
Finally, the GDPR requires consent to be unambiguous and specific, while the PD(P)O does not.



Contrary to the GDPR, the PD(P)O does not explicitly provide a legitimate interest legal basis. At most, the PD(P)O's Data Use Principle (DPP3) provides that in the case of using personal data for a new purpose, the Data User can do so if "they have reasonable grounds for believing that the use of the data for the new purpose is clearly in the interest of the data subject".

Lawfulness

Criterion 9. Conditions for the Processing of Sensitive Data



Different



Articles 9, 10, Recital 47

There are ten legal bases for processing sensitive data, subject to further additions by Member States:

1. Explicit consent.
2. To comply with obligations and exercising rights in the context of employment and social security.
3. Life protection and vital interests.
4. Legitimate activities (by a foundation, association or other non-profit body with a political, philosophical, religious, or trade union aim, which processes data about its members).
5. Establishment, exercise, or defence in legal claims.
6. Data manifestly made public by the individual.
7. Substantial public interest defined by law.
8. Preventive or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment.
9. Substantial public interest in health.
10. Archiving, scientific, or historical research purposes.

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of Data Subjects. Any comprehensive register of criminal convictions shall be kept only under the control of an official authority.

Guidance on Collection and Use of Biometric Data, Code of Practice on Consumer Credit Data, Personal Data (Privacy) Ordinance and Electronic Health Record Sharing System (Points to Note for Healthcare Providers and Healthcare Professionals)

PD(P)O 

The PD(P)O does not provide for the notion of sensitive data.

However, the Privacy Commissioner has issued guidance on enhanced requirements for certain data, including identity card numbers, personal identifiers, consumer credit data, biometric data or information relating to health, mental condition, and racial origin.

The Guidance on Collection and Use of Biometric Data (including physiological and behavioural data) provides some good practices and principles when processing biometric data.

These good practices include:

- A necessity and proportionality principle
- Data minimisation
- Privacy impact assessment
- Transparency
- Explainability
- Informed choice
- Avoidance of covert data collection
- Notice about automated decision-making
- Human intervention
- Regular and frequent purging of sensitive data
- Data accuracy
- Use limitation
- Avoidance of function creep
- Data security
- Written policy
- Staff training
- Cautious use of contractors
- Audit
- Review

Contrary to the GDPR, the PD(P)O does not provide the notion of sensitive data, nor any specific protective rules for such data.



However, the PDPC provides for certain data to be treated differently through several publications. Thus, in addition to complying with the DPPs, the Codes of Practice set out additional requirements in respect of the collection, use, retention, and deletion of specific types of personal data. Breaching a Code of Practice does not, of itself, render a Data User liable to any proceedings but evidence of such a breach is admissible in proceedings under the PD(P)O. On this point, the GDPR is more protective of sensitive data than the PD(P)O because it clearly frames and regulates the notion of sensitive data.

Lawfulness

Criterion 10. Children

35%

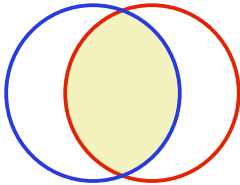
Fairly Different

<div> GDPR</div> <div>Articles 6, 8, 12, 40, 57, Recitals 38, 58, 75</div>	<div>DPP 3 (Schedule 1) and Section 2(1) of the PD(P)O</div> <div>PD(P)O </div>
<p>The GDPR doesn't define the terms "child" or "children". However, children are considered "vulnerable natural people" under the GDPR, who need special protection when it comes to their personal data.</p> <p>For delivering information society services to a child under the age of 16, the consent of a parent or guardian is necessary if the processing is based on consent. This age restriction may be lowered to 13 by EU member states.</p> <p>When children's personal data is used for marketing or gathered for information society services presented directly to children, special protection should be provided.</p> <p>Where any information is intended exclusively for a child, Data Controllers shall take necessary means to convey information relevant to processing in a brief, transparent, comprehensible, and readily available manner, using clear and simple language that the child may easily comprehend.</p> <p>In the case of information society services, the GDPR's requirements on the appropriate circumstances for processing children's data apply.</p>	<p>A person with parental authority may consent to the processing of personal data of a minor under the age of 18.</p> <p>The Privacy Commissioner recognises that children are a vulnerable group. The authority has issued guidelines on how best to handle children's personal data.</p> <p>The PD(P)O does not expressly recognise any exceptions to the collection or processing of personal data from minors.</p>

The GDPR defines specific provisions for children's data that are more protective and require the consent of their parents or guardians. On the other hand, the PD(P)O does not provide for any legal framework concerning the data of minors, except that persons with parental authority are a relevant party (without preventing minors' consent). Despite some non-binding indications from the PDPC, the GDPR is a more protective regulation for children than the PD(P)O.



Data Subjects' Rights

Criterion 11.
Transparency Requirements



63%

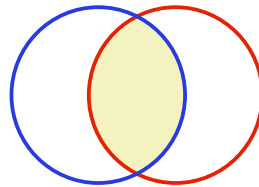
Fairly Similar

	Article 12, Recital 58	DPP5 (Schedule 1), Personal Data (Privacy) Law in Hong Kong – A Practical Guide on Compliance (point 9.10)	PD(P)O 
<p>The GDPR explicitly refers to the principle of transparency, which involves providing information to the Data Subject. The information must be “concise, easily accessible and easy to understand” through the use of “clear and simple language”.</p> <p>The information to be provided is precisely detailed in the GDPR.</p>		<p>Transparency and openness are fundamental principles of the PD(P)O, as the Openness Principle (DPP 5) clearly states.</p> <p>Data Users must ensure transparency of their policies and practices at all stages, from collection to deletion.</p> <p>What information must be provided is detailed in the PD(P)O.</p>	

The GDPR and the PD(P)O both provide transparency requirements. The PD(P)O defines transparency as a fundamental principle of personal data protection, while the GDPR includes transparency in its section dedicated to Data Subjects' rights. The GDPR produces more details on how to make information transparent than the PD(P)O. Similarly, the PD(P)O and the GDPR both precisely detail the information to provide to the Data Subject, but the GDPR is more demanding.

Data Subjects' Rights

Criterion 12. Right of Access



55%

Fairly Similar



Articles 12, 15, Recitals 59-64

Data Subjects have the right to access the personal data that is processed by a Data Controller.

According to the GDPR, the Data Controller must provide the following information when responding to an access request:

- The recipients or categories of recipients to whom the personal data has been or will be disclosed, in particular recipients in third countries or international organisations.
- The envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.
- The existence of the right to request rectification from the Data Controller.

According to the GDPR, the right of access shall not infringe on others' rights or freedoms, particularly those connected to trade secrets.

Requests from Data Subjects under this right must be responded to without "undue delay" and in any case within one month of receipt.

The right to access is unrestricted. A charge may be required in certain cases, particularly when the demands are unwarranted, unreasonable, or recurrent.

Data Subjects must be able to submit their requests in a number of ways, including verbally and by technological means. In addition, when a request is made using electronic means, the Data Controller shall respond via electronic means as well.

DPP 6 (Schedule 1), Part 5, Division 1

PD(P)O

According to the Data Access & Correction Principle (DPP6), a Data Subject is entitled to request access to personal data. The right to access can be denied if such access cannot be provided without disclosing the identity of other individuals.

The Data User is required to answer the Data Subject in writing. If the Data User is unable to comply with the request, the Data Subject must inform the individual in writing of the reasons why the Data User is so unable and to comply with the request to the extent of their ability.

Data Users have a period of 40 days to answer the request and to justify the refusal, if necessary. Failure to comply with the time limit or failure to respond constitutes an offence under the PD(P)O.

Access requests can be subject to a fee, but the price must be reasonable.

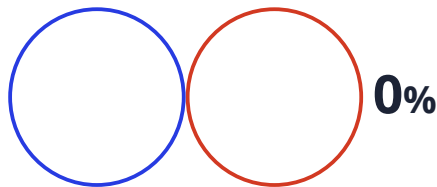
The Data User can refuse to comply with a data access request if the request is not in writing in the Chinese or English language, or if the Data User is not supplied with sufficient information to reasonably be able to locate the personal data requested.

The GDPR and the PD(P)O both provide Data Subjects with the right to access their personal data. They also both require Data Controllers to respond to this right in a limited amount of time (one month in the GDPR, 40 days in the PD(P)O).

They, however, differ in the implementation of the right to access. In the GDPR, the right to access can be requested in several ways, and is unrestricted and free. In the PD(P)O, Data Subjects should request their personal data through a written request in the Chinese or English language, and may be subject to a fee.

Data Subjects' Rights

Criterion 13. Right to Data Portability

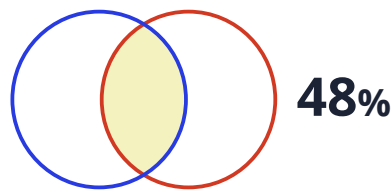


Different

The right to data portability is explicitly contained in the GDPR. This right does not seem to contain an equivalent in the PD(P)O.

Data Subjects' Rights

Criterion 14. Right to Rectification



Fairly Different



Article 16

Data Subjects have the right to correct inaccurate personal data and complete incomplete personal data.

Where personal data is updated, it must be communicated to each recipient to which it was disclosed, unless this would involve disproportionate effort.

The Data Controller must restrict processing where the accuracy of the data is disputed for the time needed to verify the request.

DPP6 (Schedule 1), Part 5, Division 2



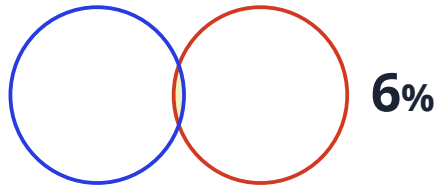
The right to rectification and the right of access are covered under DPP6, Access to Personal Data, which is also sometimes officially referred to as the "Data Access & Correction Principle". Data Subjects can address a request for correction to the Data User when they notice an error in their personal data.

The request for correction must be preceded by a request for access. If the data is incorrect, then the Data User must comply with the request without charging a fee. They have a period of 40 days to respond.

The GDPR and the PD(P)O both provide the Data Subject with the right to correct inaccurate personal data. The GDPR provides a wider right to rectification as the Data Subject is explicitly entitled to require the Data Controller to complete incomplete data. Under the PD(P)O, the Data Subject must first make an access request in order to be able to make a correction request, whereas under the GDPR, the Data Subject can directly exercise the right to rectification without any access to it. Finally, the GDPR requires the Data Controller to restrict processing when the accuracy of the data is disputed, while the PD(P)O does not provide such a requirement.

Data Subjects' Rights

Criterion 15. Right to be Forgotten / Right to Erasure



Different



GDPR

Articles 12, 17 Recitals 59, 65-66

The right to be forgotten applies to specific circumstances, such as when a Data Subject's consent is revoked and there is no other legal basis for processing, or when personal data is no longer required for the purposes for which it was obtained.

The right to exercise erasure/to be forgotten is unrestricted. However, there are certain circumstances in which a charge may be demanded, such as when demands are baseless, unreasonable, or frequent.

If the Data Controller has made personal data public and is required to erase the personal data, the Data Controller shall take reasonable steps, including technical measures, to notify controllers processing the personal data that the Data Subject has requested the erasure by such controllers of any links to, or copy or replication of those personal data, taking into account the available technology and the cost of implementation.

The GDPR sets out exceptions to the right to erasure when:

- It conflicts with freedom of speech and information.
- Compliance with public interest objectives in the field of public health.
- Creation, exercise, or defence of legal claims.
- Compliance with legal duties for a public interest purpose.

Under this right, Data Subject requests must be responded to "without excessive delay and in any case within one month of receipt of request".

Code of Practice on Consumer Credit Data

PD(P)O

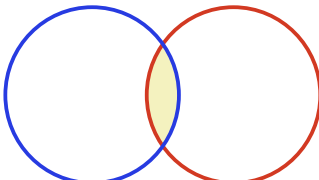
The PD(P)O does not provide for a right to be forgotten, but it contains a general obligation to delete data once it is no longer needed for the purpose for which it was used.

However, for certain data, such as banking data, the Privacy Commissioner has published a code of practice according to which Data Subjects have the right to request the deletion of their personal data from a terminated account from the Data User.

Contrary to the GDPR, the PD(P)O does not provide a right to erasure. The right to deletion of personal data is only provided towards consumer credit data in the Code of Practice dedicated to such data.



Data Subjects' Rights

Criterion 16.
Right to Object



20%

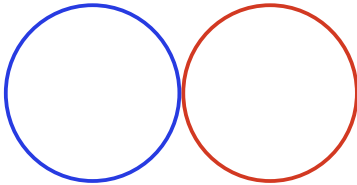
Different

<div> GDPR</div> <div>Article 21</div>	<div>Part 6A</div> <div>PD(P)O </div>
<p>Data Subjects have the right to object to the processing of their personal data if:</p> <ul style="list-style-type: none">• The processing of personal data is for direct marketing purposes, including profiling related to direct processing.• The processing of personal data is for scientific, historical research, or statistical purposes, unless processing is necessary for the performance of a task of public interest.• The processing is based on the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller, including profiling.• The processing is based on the legitimate interest of the Data Controller or third parties, including profiling. <p>The Data Controller shall no longer process the personal data unless the Data Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims.</p> <p>A request to limit the processing of personal data must be replied to promptly, and in any case, within one month of receiving the request. Due to the complexity and amount of petitions, the deadline might be extended for another two months.</p>	<p>The Data Subject does not have a general and explicit right to object to the processing of their personal data. The PD(P)O specifies that for marketing purposes, consent includes an indication of non-objection to the processing or provision of personal data.</p>

The PD(P)O provides an implicit right to object as an extension of consent in the context of direct marketing. On the other hand, the GDPR provides for the Data Subject a general right to object to the processing of personal data when it is for direct marketing, for scientific, historical or statistical purposes, for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the Data Controller, and when the processing is based on legitimate interest.

Data Subjects' Rights

Criterion 17.
Rights Related to Profiling



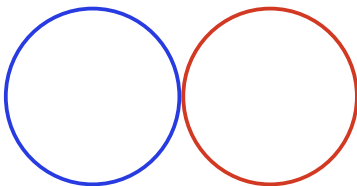
0%

Different

Rights related to profiling are explicitly contained in the GDPR. Such rights do not seem to contain an equivalent in the PD(P)O.

Data Subjects' Rights

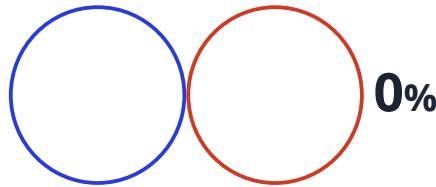
Criterion 18.
Right to Restrict the Use of the Personal Data



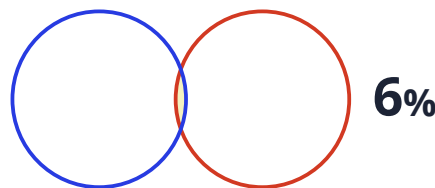
0%

Different

The right to restrict the use of the personal data is explicitly contained in the GDPR. This right does not seem to contain an equivalent in the PD(P)O.

Accountability Requirements**Criterion 19.**
Appointment of a Representative**Different**

Contrary to GDPR, there is no requirement in the PD(P)O to appoint a representative in Hong Kong.

Accountability Requirements**Criterion 20.**
Appointment of a Data Protection Officer**Different**

1 2

**Articles 38, 39****DPP 1, Privacy Management Programme – A Best Practice Guide p.39-40****PD(P)O** **Designation**

Data Controllers and Data Processors, as well as their representatives, are obliged to designate a DPO under the GDPR, in any case where:

- The processing is carried out by a public authority or body, except for courts acting in their judicial capacity.
- The core activities of a Data Controller or Data Processor consist of processing operations that, by their nature, scope, and/or purposes, require regular and systematic monitoring of Data Subjects on a large scale.
- The core activities of the consortia consist of processing on a large scale sensitive data or personal data relating to criminal convictions and offences.

A group may nominate a single DPO who must be reachable by all establishments. When a public authority or body is the Data Controller or Data Processor, a single DPO might be appointed for many public authorities or bodies, depending on their organisational structure and size.

The DPO shall be designated on the basis of professional qualities, in particular expert knowledge of data protection law and practises.

There is no formal requirement to appoint a Data Protection Officer.

DPP1, Purpose and Manner of Collection of Personal Data, requires a Data User to provide contact information for a person to whom the Data Subject's access and rectification requests should be forwarded. The Data User must provide this information before or during the collection of the Data Subject's personal data.

However, the regulator advises organisations to implement a Privacy Management Programme (PMP). Indeed, it has issued a guide in which it recommends appointing a designated officer (i.e. Data Protection Officer) "to oversee the organisations' compliance with the Ordinance and implementation of PMP".

The missions are similar to those of a DPO in the GDPR.

Tasks and responsibilities

The DPO have at least the following tasks:

- To inform/advise the Data Controller or Data Processor and monitor compliance with their obligation under GDPR and other EU/national law applying to processing.
- To provide advice and monitor performance of Data Protection Impact Assessments (DPIA).
- To cooperate and act as a contact point with supervisory authorities.

Position

The DPO must be involved in all issues relating to personal data protection, and must be provided all resources necessary to perform their tasks.

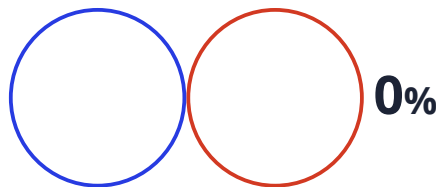
The DPO is independant and shall neither receive any instructions regarding the exercise of their tasks nor be dismissed or penalised for performing these tasks.

The DPO can fulfil other tasks and duties, but the Data Controller/Data Processor must verify that these tasks do not result in a conflict of interest.

Contrary to the GDPR, the PD(P)O does not impose a legal obligation to designate a DPO. However, appointing a DPO is strongly recommended by the supervisory authority.

Accountability Requirements

Criterion 21. Record of Processing

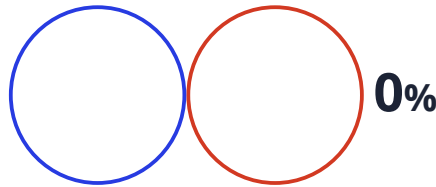


Different

Contrary to the GDPR, the PD(P)O does not impose to maintain records of processing.

Accountability Requirements

Criterion 22. Data Protection Impact Assessment (DPIA)



Different



Article 35

The GDPR requires controllers to carry out a DPIA, in particular using new technologies, when the processing is likely to result in a high risk to the rights and freedoms of natural persons.

A DPIA is particularly required in the following situations:

- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.
- Processing on a large scale of sensitive data.
- Systematic monitoring of a publicly accessible area on large scale.

At the very least, the evaluation must include the following:

- A systematic description of the proposed processing operations and lawful processing purposes.
- The need and proportionality of the operations in connection to the purposes.
- Risks to Data Subjects' rights and freedoms.

Privacy Management Programme – A Best Practice Guide p.49, Guidance on Collection and Use of Biometric Data, p.3

PD(P)O 

Privacy Impact Assessments are not mandatory, but the Privacy Commissioner has published a guide that explains when it is recommended to conduct a DPIA.

According to the Privacy Commissioner, it is important to conduct a DPIA when:

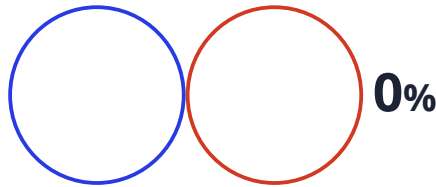
- There is a material change to the regulatory requirements relating to personal data.
- There is a material change to the organisation's existing personal data process.
- Introducing a new personal data handling process in the organisation.
- The organisation intends to engage Data Processors to handle personal data on its behalf.

It is recommended that the Data Processor carries out a DPIA when processing biometric data.

Although the Hong Kong Privacy Commissioner recommends carrying out DPIAs in some instances, there is no legal obligation to do so under the PD(P)O. In the GDPR, DPIAs are a legal requirement when Data Controllers consider setting up the processing of personal data that poses a high risk to individuals' rights and freedoms.

Accountability Requirements

Criterion 23. Privacy by Design



0%

Different



Article 25, Recital 78

At the time of the determination of the means for processing and at the time of the processing itself, the Data Controller must implement appropriate technical and organisational measures in an effective manner and must integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of Data Subjects.

When doing so, the Data Controller must take into account the state of the art, the cost of implementation, and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

Such technical and organisation measures can include pseudonymisation and data minimisation.

Guide to Data Protection by Design for ICT systems, Privacy by Design and Best Practice Guide on Mobile App Development

PD(P)O

The PD(P)O does not expressly require protection by design.

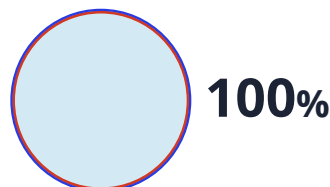
However, the Privacy Commissioner is well aware of the importance of using privacy by design. The PCPD defines the concept as “the philosophy of embedding privacy from the outset into the design specifications of accountable business processes, physical spaces, infrastructure and information technologies”.

The Privacy Commissioner has issued guidelines on privacy by design for ICT (Information and Communications Technologies) systems and mobile application development in which it details the best practices and principles related to privacy by design. These are non-binding sectoral rules.

The GDPR explicitly requires Data Controllers to implement technical and organisational measures to protect Data Subjects' rights and freedom at the design stage. On this point, while the privacy by design principle is not provided in the PD(P)O, the PCPD still has established a very detailed guide that encourages the implementation of privacy by design principles.

Accountability Requirements

Criterion 24. Audit Requirements



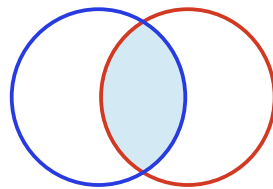
100%

Similar

Neither the GDPR nor the PD(P)O provides audit requirements. In the GDPR, audits can be completed as a way to demonstrate compliance.

Accountability Requirements

Criterion 25. Appointment of Processors



42%

Fairly Different



GDPR

Article 28

Where processing is to be carried out on behalf of a Data Controller, the Data Controller shall use only Data Processors that provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the Data Subject.

The Data Processor shall not engage with another Data Processor without prior specific or general written authorisation of the Data Controller. In the case of general written authorisation, the Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of other Data Processors, thereby giving the Data Controller the opportunity to object to such changes.

DPP 2 (Schedule 1), DPP 4 (Schedule 1)

PD(P)O

The PD(P)O only regulates the relationship between the Data User and the Data Processor through personal data retention and security requirements. A Data User is responsible for the way the Data Processor handles personal data. It must use contractual means or safeguards to ensure that personal data is protected from collection to deletion and that the processor complies with the PD(P)O.

The Privacy Commissioner has given recommendations regarding the type of contractual obligations that the Data User should have with the Data Processor.

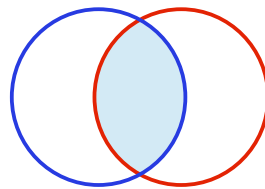
GDPR provisions apply to both Data Controllers and Data Processors. Data Controllers are required to verify that their Data Processor provides sufficient guarantees to comply with personal data protection rules, and require an agreement to be signed specifying the aim for entrusting the data, the time limit, the manner of processing, the categories of personal information, the protective measures, and the parties' respective rights and obligations.

Contrary to the GDPR, the PD(P)O does not regulate Data Processors' activities. However, Data Users are held responsible for the actions of their Data Processors, and they shall be bound by contractual terms to the Data Users' requirements in terms of personal data protection. The Privacy Commissioner recommends a list of standard contractual clauses to better frame this relationship, but they are not binding.

The reform project envisages increasing the liability of subcontractors. Inspired by foreign legislation, the government wants to create a legal framework for processors by imposing obligations on them. They would thus be responsible for the way they process and store the personal data entrusted to them by Data Users.

Accountability Requirements

Criterion 26. Information Security



53%

Fairly Similar



Article 32

Data Controllers and Data Processors are required to implement appropriate technical and organisational measures to protect the security of personal data, taking into account:

- The state of the art.
- The cost of implementation.
- The nature, scope, context and purpose of processing.
- The risk for the rights and freedoms of natural persons (depending on their likelihood and severity).

Security measures include:

- Pseudonymisation and encryption.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

DPP4 (Schedule 1)



The PD(P)O requires Data Users to take all practicable steps to ensure that any personal data they hold or process is protected against unauthorised or accidental access, processing, loss, erasure, or use.

The Data User shall have particular regard to:

- The nature of data and the harm that could result from a data breach.
- The physical location where the data is stored, and any security measures incorporated into any equipment in which the data is stored.
- Any measures taken to ensure the integrity, prudence and competence of persons having access to the data.
- Any measures taken to ensure the secure transmission of data.

The PCPD requires Data Users to implement practical measures to protect personal data from unauthorised or accidental access, loss, processing, deletion, or use.

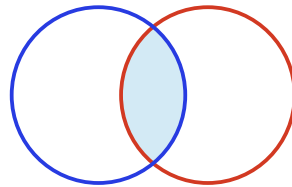
Data Users must take into account the nature of the data. The Data Processor must comply with security requirements.

The PCPD has recommended that Data Users encrypt their electronic data.

The GDPR and the PD(P)O both require Data Controllers (Data Users in the PD(P)O) to implement security measures. However, the GDPR seems to be more demanding in terms of security than the PD(P)O because it requires the Data Controller to choose their security measures according to specific criteria. Moreover, the PD(P)O does not require any DPIA to be carried out and does not provide any security measures requirements for Data Processors.

Accountability Requirements

Criterion 27. Breach Notification



32%

Fairly Different



Article 33, Article 34

The GDPR requires the Data Controller to inform without undue delay (and when feasible not later than 72 hours after becoming aware of the breach) the appropriate supervisory authority in the event of a data breach, unless the personal data breach is unlikely to pose a danger to the Data Subject. The processor must notify the controller without undue delay after becoming aware of a personal breach.

When a personal data breach is likely to result in a high risk, the Data Controller must inform the Data Subjects implicated as soon as possible.

The notification must include at a minimum:

- A description of the nature of the breach, including, where possible, the categories and approximate numbers of Data Subjects affected, as well as the categories and approximate numbers of personal data records affected.
- The DPO or another contact point's contact details.
- The likely consequences of the breach.
- Measures taken or proposed to mitigate the possible adverse effects.
- The reason for the breach.

Guidance on Data Breach Handling and the Giving of Breach Notifications

PD(P)O

There is no legal notification obligation regarding data breaches, however, there are good practices in this area. Indeed, the PCPD has issued a Guidance on Data Breach Handling and the Giving of Breach Notifications (Revised 2019).

If the Data User decides to notify the breach to the PCPD, it must use the Data Breach Notification Form created by the PCPD.

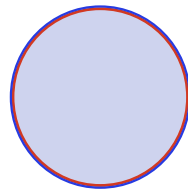
The Data Breach Notification Form includes:

- Information about the person giving the notification (i.e. the Data User).
- Details about the data breach.
- Measures taken and to be taken to contain the breach.
- The potential damages suffered.
- Advice offered to individuals.
- If the breach has been notified to other bodies, regulators, or law enforcement.

Contrary to the GDPR, the PD(P)O does not include a legal obligation for the Data User to notify the Privacy Commissioner about a data breach. The Privacy Commissioner has established a guidance note, however, this notice is not binding. The elements communicated in the Data Breach Notification Form recommended by the Privacy Commissioner are similar to those of the GDPR. In January 2020, the Government proposed PD(P)O amendments (that are not adopted yet) to make the Data Breach Notification Mechanism mandatory. In such a case, the Data User would be required to report breaches having a real risk of significant harm both to the PDPC and impacted individuals.

Data Localisation and Transfer

Criterion 28. Data Localisation Requirements



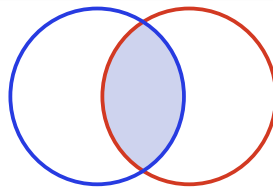
100%

Similar

Neither the GDPR nor the PD(P)O provide data localisation requirements.

Data Localisation and Transfer

Criterion 29. International Data Transfer



46%

Fairly Different

Similarity score if Section 33 enters into force



GDPR

Articles 5, 44-50

The GDPR enables personal data to be transferred to a third country or international organisation that meets the EU Commission's criteria for adequate data protection.

In the absence of an EU Commission's adequacy decision, transfers to third countries or international organisations are allowed if it is based on binding appropriate safeguards, including binding corporate rules.

In the absence of an EU Commission's adequacy decision and binding appropriate safeguards, the transfer is authorised, by derogation, in the following cases:

- The Data Subject has explicitly consented to the transfer after having understood the risk of such transfer due to insufficient safeguards.
- The transfer is necessary for the performance of a valid contract between the Data Subject and the Data Controller.
- The transfer is necessary for the conclusion or performance by the Data Controller and other persons of a valid contract that is in the interest of Data Subject.
- The transfer is necessary for important reasons of public interest.
- The transfer is necessary for establishment, exercise or defence of legal claims.

Part 6, Section 33

PD(P)O

The PD(P)O contains a provision for cross-border transfers that is not yet effective.

This provision prohibits the transfer of personal data outside Hong Kong, except when:

- The Commissioner has issued a notice stating that there are reasonable grounds for believing that there is a law which is substantially similar to, or serves the same purposes as, the PD(P)O in force in a jurisdiction outside Hong Kong.
- The Data User has reasonable grounds for believing that there is a law which is substantially similar to, or serves the same purposes as, the PD(P)O in force in that jurisdiction.
- The Data Subject has consented in writing to the transfer.
- The transfer is for the avoidance or mitigation of adverse action against the Data Subject.
- The data is exempt from DPP3, Use of Personal Data (similar to the purpose limitation contained in DPP1).
- The Data User has taken all reasonable precautions and exercised all due diligence to ensure that the data will not, in that place, be collected, held, processed or used in any manner which would be considered a contravention of a requirement under the PD(P)O.

The Privacy Commissioner has published a guide

- The transfer is necessary to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent.

- The transfer (only to the extent laid down by the law) is made from a register which according to the law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest.

The transfer is also authorised in an *ad hoc* way if it is not repetitive, concerns a limited number of persons and is necessary for the purposes of compelling legitimate interests pursued by the Data Controller which are not overridden by the interest, rights and freedoms of Data Subjects.

on the protection of personal data in the context of transborder data transfers. This guide is informative and non-binding.

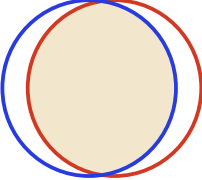
The GDPR prohibits transfers outside the EU unless the Commission has issued an adequacy decision that the Data Controller can rely on about adequate safeguards, or if a derogation applies.

The PD(P)O also provides some rules about transfers outside Hong Kong, but these provisions have not yet come into force. If Section 33 comes into force, the PD(P)O will also prohibit out-of-territory transfers unless certain conditions are met. Some of these conditions are similar to the GDPR: the Data User can rely on an adequacy decision issued by the Commissioner or on the Data Subject's consent.

Contrary to the GDPR, the PD(P)O does not allow transfers on the basis of appropriate safeguards, or the other derogations of the GDPR. However, the PD(P)O provides a wide ability for the Data User to justify the transfer on its own assessment of the third country's data protection level or on due diligence grounds. Contrary to the GDPR, the PD(P)O also allows transfer when the processing is for the avoidance or mitigation of adverse action against the Data Subject or when the data is exempt from the DPP3, Use of Personal Data (similar to the purpose limitation contained in DPP1).



Enforcement

Criterion 30.
Data Protection Authority



88%

Similar

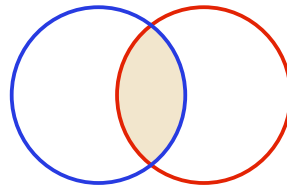
<div> GDPR</div> <div>Articles 31, 51-59</div>	<div>Section 5(1), Parts 2, 7</div> <div>PD(P)O </div>
<p>The supervisory authorities have the jurisdiction to:</p> <ul style="list-style-type: none">• Require the Data Controller or Data Processor to bring processing activities into accordance with the GDPR's rules, when applicable, in a particular way and within a set term.• Apply a temporary or permanent restriction, such as a processing prohibition. <p>In accordance with EU or Member State procedural law, the supervisory authorities have the authority to:</p> <ul style="list-style-type: none">• Order the Data Controller and Data Processor to provide any information required for the performance of their tasks.• Obtain access to any premises of the Data Controller and Data Processor, including any data processing equipment and means. <p>The supervisory authorities also have the jurisdiction to reprimand and give warnings, and to require the correction or deletion of personal data, and apply administrative penalties.</p> <p>The supervisory authorities have investigative rights, including the ability to conduct data protection audits, evaluate issued certificates, and alert the Data Controller or Data Processor of a suspected GDPR violation.</p> <p>The GDPR explicitly states that each supervisory authority must carry out its responsibilities and wield its powers independently.</p> <p>The GDPR is silent on the source of funds that must be made available to regulatory bodies. In this case, the Member State has complete choice over the source of financing.</p>	<p>The Data Protection Authority is called the Office of the Privacy Commissioner for Personal Data (PCPD) and is responsible for monitoring, supervising, promoting and enforcing the provisions of the Personal Data (Privacy) Ordinance (PD(P)O). The PCPD was created specifically to enforce the PD(P)O. The PCPD's powers were further expanded by an amending ordinance in 2021.</p> <p>The Privacy Commissioner has a great training and educational role since it compensates for the failures of the PD(P)O on many occasions. There is no legal requirement to notify the Privacy Commissioner in respect of any collection or use of personal data.</p> <p>The Privacy Commissioner has the authority to carry out inspections of Data Users, including their personal data systems. The Privacy Commissioner also has advisory missions in terms of personal data legislations, and shall work on certifications.</p> <p>The PCPD is an independent body which can sue and be sued by Data Users.</p> <p>To combat doxxing, the PCPD may request assistance and materials from any person upon written notice, apply for a warrant to search premises and collect evidence, and arrest and search any person who may have committed acts of doxxing.</p>

The GDPR's supervisory authorities and the PDPC share a lot of similarities. The Office of the Privacy Commissioner for Personal Data (PCPD) is an independent body set up to monitor the PD(P)O's compliance with investigatory, advisory and certification powers.

The Privacy Commissioner has a great training and educational role since it completes the failures of the PD(P)O on many occasions. The PCPD has a great power of interpretation and recommendation as an authority similar to that of GDPR.

Enforcement

Criterion 31. Penalties



40%

Fairly Different



Article 83

Supervisory bodies may issue rules that include additional factors for calculating the monetary penalty amount. The GDPR allows for sanctions to be imposed on government entities. The creation of laws for the application of administrative fines to public agencies and organisations is left to Member States.

Depending on the infraction, the penalty may be:

- Up to 2% of worldwide annual revenue or €10 million, whichever is greater.
- 4% of global annual turnover or €20 million, whichever is greater.

Part 9



Regulators and law enforcement can apply civil and criminal penalties and administrative remedies.

A table exists that summarises the various offences under PD(P)O and the respective penalties.²

The maximum financial penalty concerns the field of marketing, it amounts to a fine of HK\$1,000,000 and five years imprisonment.

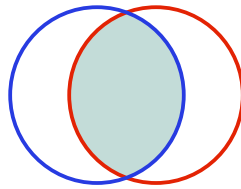
Private remedies may be pursued. For this, individuals can file complaints with the PCPD or initiate civil proceedings against a Data User to obtain compensation.

The fines are much higher under the GDPR than under the PD(P)O. The GDPR also provides for monetary penalties that are proportionate to business revenues, while the PD(P)O does not. However, in January 2020, the Government announced that it is considering increasing the administrative fine and is, in particular, “exploring the feasibility of introducing an administrative fine linked to the annual turnover of the data user”.

² https://www.pcpd.org.hk/misc/files/table2_e.pdf

Exemptions

Criterion 32. Anonymised Data



63%

Fairly Similar



Recital 26

The GDPR does not apply to data that has been “anonymised”, meaning that it can no longer be used to identify the Data Subject.

Section 2

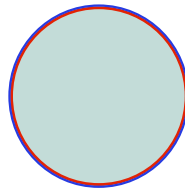


The definition of personal data does not seem to include anonymised data.

Neither the GDPR nor the PD(P)O apply to anonymised data.

Exemptions

Criterion 33. Social Media Intermediaries and Identity Management



100%

Similar

Neither the GDPR nor the PD(P)O include provisions in terms of social media intermediaries and identity management.



However, it is worth noting that in Hong Kong, the Privacy Commissioner has issued guidelines on the subject called, “Guidance on Protecting Personal Data Privacy in the Use of Social Media and Instant Messaging Apps”. Social media and instant messaging apps are widely used by people in Hong Kong. However, their use carries inherent yet non-negligible risks to the user’s privacy in relation to personal data. This Guidance aims to highlight those risks and provide practical advice that will help to mitigate the risks.

Exemptions

Criterion 34.
Exemptions for Research

55%

Fairly Similar

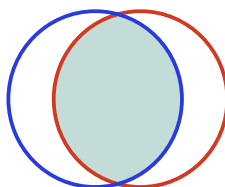
<div> GDPR</div> <div>Articles 5, 9, 14, 17, 89 Recitals 33, 156, 159-161</div>	Section 62	PD(P)O 
<p>Personal data processing for research purposes is governed by specific standards under the GDPR.</p> <p>Processing of sensitive data is not prohibited under the GDPR when it is “necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, which shall be proportionate to the goal pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and interests of the Data Subject”.</p> <p>According to the GDPR, special categories of personal data that require extra protection should only be processed for health-related purposes when absolutely necessary to achieve goals for the benefit of natural persons and society as a whole, such as in the context of public health studies.</p> <p>The GDPR states that the processing of personal data for scientific research objectives should be construed “in a comprehensive way,” including “technological development and demonstration, basic research, applied research, and privately sponsored research”, among other things.</p> <p>Under the GDPR, Member States may derogate from some Data Subjects’ rights, such as the right to access, the right to rectification, the right to object, and the right to restrict processing, if such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the achievement of those purposes.</p>	<p>The PD(P)O provides for exceptions from certain compliance requirements. These include, for example, the prevention or prosecution of crime, security and defence, statistics and research, current events, protection of the health of a Data Subject, etc.</p> <p>Personal data processing for research purposes is exempt from the provision of DPP3, Use of Personal Data. It means that data collected can be reused for the purpose of research without the consent of the Data Subject or the relevant person. Processing for research purposes must comply with the other provisions of the PD(P)O.</p>	

Both laws provide special derogation for processing personal data for research purposes. In the GDPR, the exemptions are particular to the situation where they are needed and the principle of necessity of the derogation is the cornerstone of these derogatory rules. The GDPR also provides that the Data Controller must be particularly cautious when processing personal data for research purposes because of these derogations.

On the other hand, the PD(P)O’s exemptions are more general. The processing of personal data for research purposes must comply with the PD(P)O, except for the Use of Personal Data, DPP3, which implies that personal data collected can be reused for research purposes without the consent of the Data Subject.

Exemptions

Criterion 35. Application to Public Authorities



74%

Fairly Similar



GDPR

Article 2

The GDPR is not applicable to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Part 8

PD(P)O 

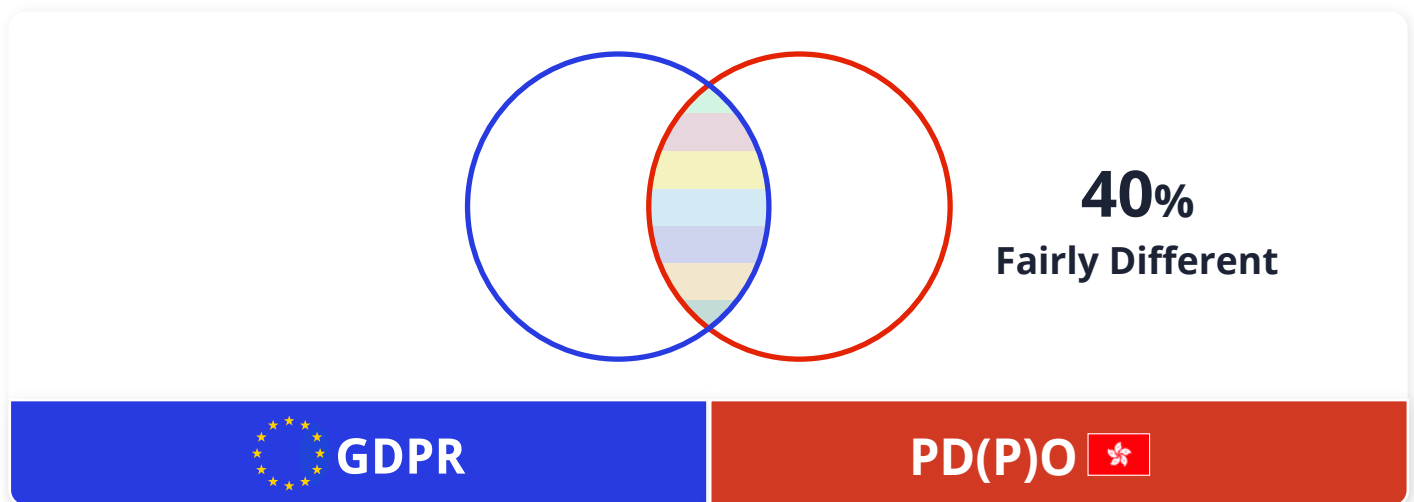
The PD(P)O is applicable to both the private and the public sectors.

The PD(P)O exempts from all or part of its provisions:

- The performance of judicial functions.
- Security activities in respect of Hong Kong.
- The prevention and detection of crime.
- Protected product and relevant records under the Interception of Communications and Surveillance Ordinance.
- Health.
- Care and guardianship of minors by the Hong Kong Police Force or Custom and Excise Department.
- The exercise of legal professional privilege, self-incrimination, and legal proceedings.
- Journalistic activities.
- Transfer of records to the Government Records Service.

The GDPR is not applicable to personal data processing for law enforcement activities. The PD(P)O does not include such an exemption; instead it exempts from all or part of its provisions some processing that may be carried out by the public sector. For instance, security activities are not exempted from all the PD(P)O's provisions but only from some principles and rules.

Conclusion



The PD(P)O and the GDPR are fairly different. Therefore, doing business in the European Union and in Hong Kong requires an important privacy gap analysis effort for companies.

The PD(P)O was issued at the same time as the European Directive 95/46, and came into force just before Hong Kong was returned to China. It was one of the first Asian global privacy laws. However, the Hong Kong government's inaction in updating and enforcing its provisions makes Hong Kong's privacy protection less effective than most other Asian countries³. For instance, the provisions about international transfers are still not in force 17 years after the adoption of the PD(P)O.

Inspired by the GDPR and the national data protection frameworks of Australia, Canada, New Zealand, and Singapore, in 2020, the Hong Kong Government proposed several amendments in order to update the PD(P)O. Among these amendments, the government proposes to:

- Create a mandatory Data Breach Notification Mechanism.
- Require Data Users to formulate a clear retention policy.
- Increase administrative fines, including fines linked to the annual turnover of the Data User.
- Directly regulate Data Processor's processing activities.
- Explicitly refer to "identifiable persons" in the definition of personal data.
- Regulate doxxing.

For now, the PD(P)O's only adopted amendment has been to cope with doxxing activities.

Because Hong Kong does not have updated privacy laws yet (in terms of international transfers, data breaches, etc.), companies established in Hong Kong will have to comply with foreign privacy laws that have extraterritorial effects. It is notably the case for the provisions of the Chinese PIPL, which are more demanding than those of the PD(P)O.

³ Charles Mok, "The Downfall of Hong Kong's Privacy Law" (2021), The Diplomat, <https://thediplomat.com/2021/09/the-downfall-of-hong-kongs-privacy-law/>

Compliance-as-Code: Our Solution

As this report highlights, there is a growing list of data protection compliance requirements around the world, with new laws and legislative requirements in place to assess how personal data or PII (Personal Identifiable Information) is being managed by companies.

Compliance is critical to every business: if you are not compliant with industry regulations, at best, you risk a fine and a bad reputation amongst your ecosystem and customers. At worst, you could be forced to shut your doors and stop trading completely.

At ALIAS, we work with companies and organisations of all sizes to help build in a compliance-as-code approach. Our APIs enable automated compliance: our PII Storage Duration API, for example, regularly assesses stored datasets to ensure that they meet regulatory requirements for the length of time data can be stored by a company.

By implementing compliance at the code level, you are able to automate regulatory prevention and monitoring, in order to increase your compliance coverage over time to 100%, with real-time feedback, and maintain oversight at 100%. This is what we call the DevRegOps approach.

In terms of Data Protection, what is Compliance-as-Code?

Data protection compliance-as-code refers to the tools and practices that allow you to embed the three core activities at the heart of compliance, at the code level of your organisation's tech stack:

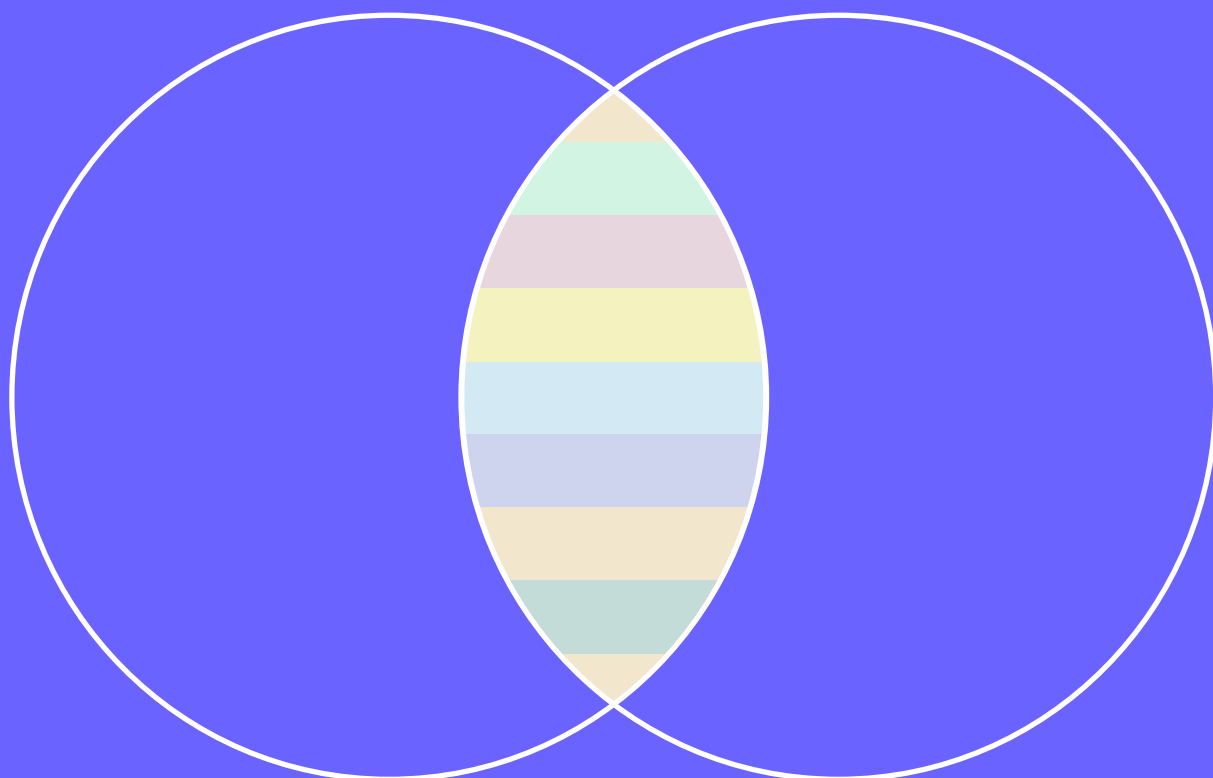
✓ Detect

✓ Solve

✓ Prevent

Contact us for a demo of our tools and to discuss implementing compliance-as-code solutions for your business.

Sign up to our [privacy newsletter](#) to receive information about changing legislations and news regarding data privacy protections.



www.gdpr.dev