



GDPR VS THE WORLD

PART 1 GDPR VS ASIA



Thailand

Malaysia 

China

Hong Kong

Japan

Singapore

India

South Korea

Indonesia

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



Stéphanie Exposito-Rosso
IT Legal Expert and Main Author



Sumedha Ganjoo
Legal Research Lead



Katia Bouslimani
Chief Legal Research Officer



Adam Ali-Bey
IT Legal Expert



Antoine Piquet
IT Legal Expert



Eloïse Quinzin
IT Legal Expert

We would like to thank Bianca Kunrath, Era Selmani and Ylli Kodza for their feedback. Copy editing, report design, and support for content strategy was provided by platformable.com

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 August 2022. Note that the regulation is meant to evolve.

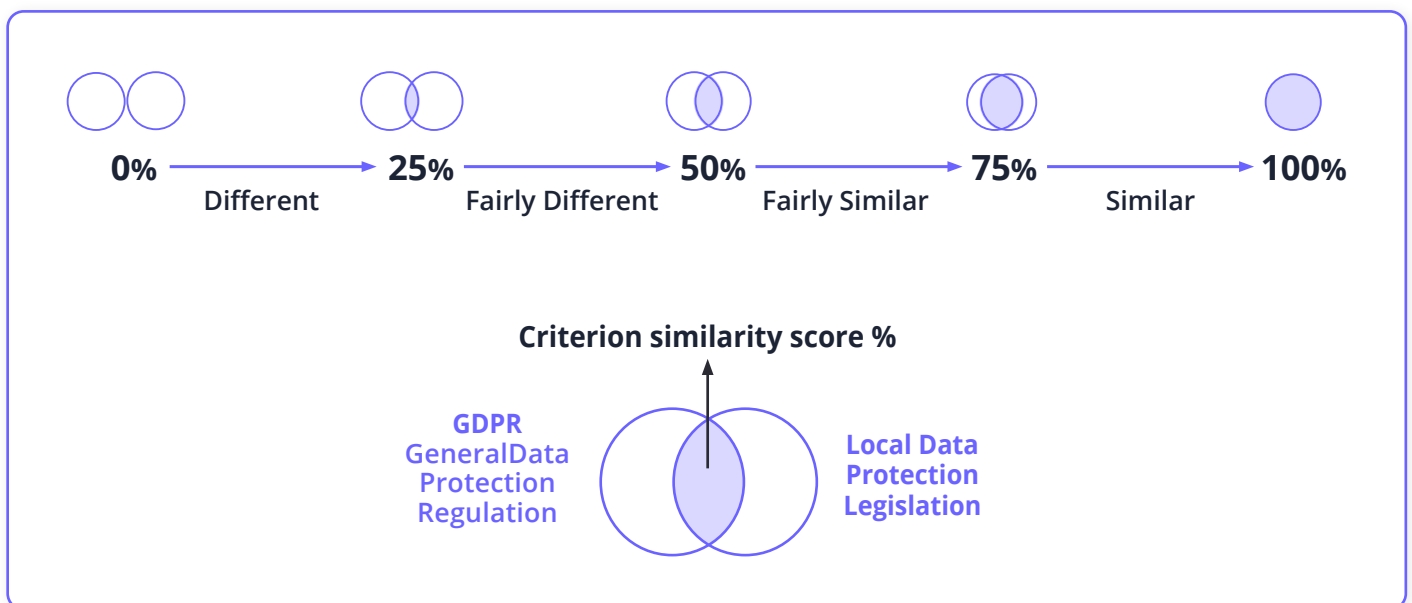
Published September 2022

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:



35 Criteria
divided into
7 Categories

■ Scope	Criteria 1–5 ●●●●●
■ Lawfulness	Criteria 6–10 ●●●●●
■ Data Subjects’ Rights	Criteria 11–18 ●●●●●●●●
■ Accountability Requirements	Criteria 19–27 ●●●●●●●●●
■ Data Localisation and Transfer	Criteria 28–29 ●●
■ Enforcement	Criteria 30–31 ●●
■ Exemptions	Criteria 32–35 ●●●●

Content

05 List of Acronyms

06 Introduction

08 Scope

Criterion 1. The Territorial Scope /8

Criterion 2. The Subject Matter Scope /9

Criterion 3. Definition of Personal Data /11

Criterion 4. Definition of Sensitive Personal Data /12

Criterion 5. Relevant Parties /13

15 Lawfulness

Criterion 6. Legal Bases /15

Criterion 7. Consent /16

Criterion 8. Legitimate Interest /17

Criterion 9. Conditions for Processing of Sensitive Data /17

Criterion 10. Children /19

20 Data Subjects' Rights

Criterion 11. Transparency Requirements /20

Criterion 12. Right of Access /21

Criterion 13. Right to Data Portability /22

Criterion 14. Right to Rectification /22

Criterion 15. Right to be Forgotten / Right to Erasure /23

Criterion 16. Right to Object /24

Criterion 17. Rights Related to Profiling /25

Criterion 18. Right to Restrict the Use of the Personal Data /25

26 Accountability Requirements

Criterion 19. Appointment of a Representative /26

Criterion 20. Appointment of a DPO /26

Criterion 21. Record of Processing /27

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

41 Compliance-as-Code: Our Solution

List of Acronyms

D

DPO: Data Protection Officer

DPIA: Data Protection Impact Assessment

G

GDPR: General Data Protection Regulation

J

JPDP: Jabatan Perlindungan Data Peribadi (Department of Personal Data Protection)

P

PDPA : Personal Data Protection Act

PDPC : Personal Data Protection Committee

Introduction

Malaysia is a strong economic partner to the EU. E-commerce is rising and is now at the core of the country's economy. As such, commercial relationships are tight and the transfer of information cannot be avoided.

Before analysing the Malaysian data protection framework, it is important to note that there is no definition of the term "privacy" in Malaysia's Personal Data Protection Act (PDPA). There is some relevant terminology to make the law clear in terms of understanding and application, such as personal data, sensitive personal data, Data Subject, processing, Data Processor, and Data User, but there is no definition of the core concept of privacy.

Moreover, there are no explicit provisions for privacy in the Constitution of Malaysia.¹ The courts have been reluctant to enshrine a right to privacy, and despite the government's need to enact a data protection law in Malaysia, it took nearly 20 years for the PDPA to come into effect.

It seems that, as the Secretary-General of the Ministry of Energy, Communications and Multimedia, Datuk Noraizah Abdul Hamid declared, the PDPA was based on OECD guidelines, the EU directives, and the UK, Hong Kong, and New Zealand models.

The Personal Data Protection Act 2010 (PDPA) came into force on 15 November 2013. It sets out a comprehensive cross-sectoral framework for the protection of personal data in relation to commercial transactions.

Prior to 2010, the regulation of personal data was governed mainly by industry-specific legislation. Data protection obligations were spread out among certain sectoral secrecy and confidentiality obligations, while personal information was primarily protected as confidential information through contractual obligations or civil actions for breach of confidence.²

Alongside the PDPA, five pieces of subsidiary legislation were also enforced on 15 November 2013. Based on the subsidiary legislation, the Personal Data Protection Commissioner ("the Commissioner") was appointed and rules were determined to supervise the registration of Data Users and the fines that may be imposed under the PDPA. This subsidiary legislation was passed simultaneously in order to facilitate the enforcement of the PDPA.

To date, numerous other laws have been passed, including: the Personal Data Protection Regulations 2013 ("the 2013 Regulations"), the Personal Data Protection (Class of Data Users) Order 2013 ("the Order"); the Personal Data Protection (Registration of Data User) 2013 ("Registration Regulation"); the Personal Data protection (Fees) Regulations 2013; the Personal Data Protection (Compounding of Offences) Regulations 2016 ("Compounding of Offences Regulations"); the Personal Data Protection (Class of Data Users) (Amendment) Order 2016 ("the Order Amendment"); and the Personal Data

¹ Md. Toriqlul Islam, "A brief historical account of global data privacy regulations and the lessons for Malaysia", *Sejarah: Journal of History*

² Shanthi Kandiah, "The Privacy, Data Protection and Cybersecurity Law Review: Malaysia" (2021), *The Law Reviews*, <https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/malaysia>

Protection (Appeal Tribunal) Regulations 2021. Besides the numerous legislations, standards, and codes of practice have also been issued by the Commissioner. The Commissioner has issued the Personal Data Protection Standards 2015 (“the 2015 Standards”), which came into force on 23 December 2015. The 2015 Standards include security standards, retention standards, and data integrity standards which apply to personal data that is processed electronically and non-electronically. They are intended to be “a minimum requirement” and will apply to all Data Users, meaning any person who processes, has control of, or allows the processing of any personal data in connection with a commercial transaction.

Later, in 2017, the Commissioner finalised and registered four codes of practice: The Code of Practice for the Banking and Financial Sector 2017; the Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017; The Code of Practice on Personal Data Protection for the Insurance and Takaful Industries in Malaysia 2017; and the Personal Data Protection Code of Practice for the Communications Class Data Users 2017.

Finally, in February 2020, the Ministry of Communication and Multimedia issued Consultation Paper No. 01/2020 – Review of the Personal Data Protection Act 2020 (PC01/2020) on 14 February 2020, soliciting public input and comments on 22 issues raised in the PC01/2020. This document is part of an ongoing review of the PDPA.

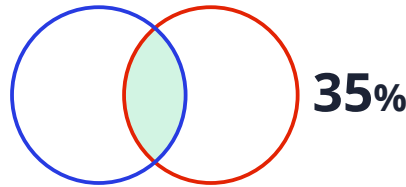
Significant revisions to the Malaysian Personal Data Protection Act 2010 (“PDPA”) will be submitted to the Malaysian Parliament in October 2022 for approval. These suggestions will impose additional requirements on both data consumers and data processors. Like the GDPR, the PDPA’s goal was to strengthen consumer confidence in electronic commerce and business transactions in the context of the rising cases of credit card fraud, identity theft, and selling of personal data without customer consent. The underlying idea was to give residents greater control over their personal and sensitive data. The PDPA is based on a set of data protection principles akin to that found in the Data Protection Directive 95/46/EC of the European Union, and for this reason, the PDPA is often described as European-style privacy law.³

It is interesting to note that the PDPA contains a certain tolerance for government surveillance activity as it does not constrain government access to personal data. In February 2021, in accordance with the Malaysian Digital Economy Blueprint, the Malaysian Government highlighted the significance of supporting smooth and secure data flows for the growth of Malaysia’s digital economy and declared its intention to review and revise the PDPA by 2025. This was reaffirmed in the Prime Minister’s presentation of the Twelfth Malaysia Plan (2021-2025) in September 2021.

³ Olivia Tan Swee Leng, Rossanne Gale Vergara and Shereen Khan, “Digital Tracing and Malaysia’s Personal Data Protection Act 2010 amid the COVID-19 Pandemic” (2021), 1 Asian Journal of Law and Policy 47-62 <https://doi.org/10.33093/ajlp.2021.3>

Scope

**Criterion 1.
The Territorial Scope**



Fairly Different

GDPR 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.

Sections 2, 3 **PDPA**

The PDPA applies to personal data processed in Malaysia.

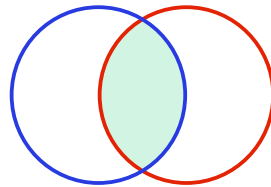
Extraterritorial scope: The PDPA does not apply to a Data User who is not established in Malaysia unless that person uses equipment in Malaysia to process personal data, other than for the purpose of transit through Malaysia. The PDPA also applies if the personal data processed outside of Malaysia is intended to be further processed in Malaysia.

Contrary to the GDPR, which determines the territorial scope in accordance with the localisation of the establishment of the controller, the territorial scope of the PDPA is triggered by the localisation of the processing in Malaysia.

The GDPR and the PDPA also differ in terms of extraterritorial scope. The PDPA’s extraterritorial scope criterion is narrower as it is triggered by the use of equipment in Malaysia to process personal data (except for the sole purpose of transit through Malaysia) or the intention of further processing in Malaysia contrary to the GDPR, which is triggered by the offering of goods and services to European Data Subjects and the monitoring of their behaviour.

Scope

**Criterion 2.
The Subject Matter Scope**



50%

Fairly Similar

 **GDPR** **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.

Sections 4, 45 **PDPA** 

The law does not mention the objective of the law, but on the Malaysian Department of Personal Data Protection website, it says that "the main objective of this law is to regulate the processing of personal data by the user in a commercial transaction data and protect personal data of common interest".

If the data is processed or intended to be processed wholly or partly by means of equipment operating automatically, in respect of a commercial transaction, and is part (or intended to be part) of a filing system, then the PDPA applies. It seems that the PDPA does not apply to anonymous data.

The PDPA exempts the processing of personal data by an individual for the sole purpose of an individual's personal, family or household affairs, including recreational purposes.

The PDPA also exempts from the application of some of its provisions:

- Processing for the purpose of prevention or detection of crime for the purpose of investigations; apprehension or prosecution of offenders; and assessment or collection or any tax or duty or any other imposition of a similar nature.
- Processing for preparing statistics or carrying out research.
- Processing necessary for the purpose of or in connection with any order or judgement of a court.
- Processing for the purpose of discharging regulatory functions.
- Processing for the sole purpose of journalistic, literary, or artistic purposes under conditions.
- Processing in relation to information on the physical or mental health of a Data Subject if the application of the Act is likely to cause serious harm to the physical or mental health of the Data Subject or any other individual.

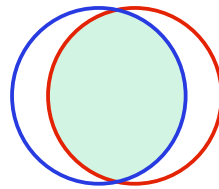
While the objectives of the GDPR are clearly stated in its provisions, the PDPA does not include any provision about such objectives. The GDPR and the PDPA both protect personal data in the economic environment, but the semantics of the objectives differ as the GDPR protects personal data as *human rights*, and the PDPA protects personal data as *common interest*.

The GDPR's subject matter application is wider than the PDPA's. Both the GDPR and the PDPA apply to personal data that is part of a file system, but the PDPA applies only to processing by automated means in respect of commercial transactions. Meanwhile, the GDPR applies to personal data regardless of the use and includes in its scope data processed by non-automated means.

The subject matter scope of both the GDPR and the PDPA excludes processing for the sole purpose of domestic reasons. They also both provide special rules for law enforcement, national security (the GDPR excludes these purposes from its scope as they are ruled by the law enforcement directive), artistic expression, statistics, journalism, and research. The PDPA also provides specific rules for some additional processing, such as information relating to physical or mental health, taking into account the risks resulting from the non-disclosure of such data.

Scope

**Criterion 3.
Definition of Personal Data**



80%

Similar

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

Section 4. Personal Data Protection Code of Practice, Part 1, Section 3.5 **PDPA** 

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.

Under the PDPA, information in respect of a commercial transaction is considered as personal data if it fulfils all of these criteria:

- It is processed by automated methods.
- It is of a file or intended to be part of a file.
- It relates directly or indirectly to a Data Subject, who is directly or indirectly identified or identifiable from that information.

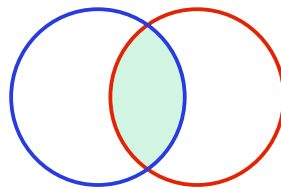
For licensees under the Communication and Multimedia Act, the Personal Data Protection Code of Practice applies to the processing of personal data that is processed in a non-automated way.

The core definition of personal data is similar in the GDPR and the PDPA. It is defined as information relating directly or indirectly to a Data Subject who is directly or indirectly identified or identifiable from that data. However, the GDPR’s definition of personal data is broader than that of the PDPA because it encompasses any personal data processed by non-automated means, while the PDPA only applies to personal data with respect to a commercial transaction that is processed by automated means.

Nevertheless, for licensees under the Communication and Multimedia Act, the Personal Data Protection Code of Practice applies to the processing of personal data that is processed in a non-automated way.

Scope

**Criterion 4.
Definition of Sensitive
Personal Data**




44%

Fairly Different

GDPR **Article 9**

The GDPR's definition of sensitive personal data covers:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- The processing of genetic data and biometric data for the purpose of uniquely identifying a natural person
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation

Section 4 **PDPA** 

Sensitive personal data means any personal data consisting of information as to the physical or mental health or condition of a Data Subject, their political opinions, religious beliefs or other beliefs of a similar nature, the commission or alleged commission by them of any offence, or any other personal data.

The PDPA also includes in the definition of sensitive personal data "any other data determined by the Minister of Communications and Media", but it does not seem that the Minister has published any.

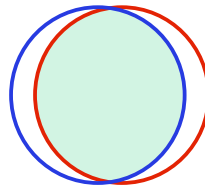
Both the GDPR and the PDPA include political opinions, religious beliefs or other beliefs of a similar nature ("philosophical beliefs" in the GDPR) and data related to the physical or mental health of a Data Subject in their definitions of sensitive personal data. The GDPR provides a wider definition of sensitive personal data as it also includes racial or ethnic origins, trade union membership, processing of genetic and biometric data for the purpose of uniquely identifying a natural person, and data concerning a Data Subject's sex life or sexual orientation.

The PDPA provides that personal data relating to the commission or alleged commission by the Data Subject is defined as sensitive personal data. Similarly, the GDPR provides that personal data relating to criminal convictions and offences or related security measures require a special legal regime, but in the GDPR the rules applying to such data are stricter than that under PDPA.

Contrary to the GDPR, the PDPA allows the Minister of Communications and Media to determine other data that can be considered as sensitive personal data. The Minister does not seem to have determined any other sensitive personal data yet.

Scope

**Criterion 5.
Relevant Parties**



88%

Similar

 **GDPR** **Articles 4 (7), 28, 30, 82**

Sections 4, 9, 11, 44  **PDPA**

- 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.

- A Data User is a person who, either alone or jointly or in common with other persons, processes personal data or has control over or authorises the processing of personal data.

- A Data Processor is a person who processes the personal data solely on behalf of the Data User and does not process the personal data for any of their own purposes.

Data Users must ensure that the personal data is accurate, complete, not misleading and kept up to date, having regard to the purpose, including any directly related purpose, for which the data was collected and further processed.

The PDPA requires Data Users to keep and maintain a record of any application, notice, request or any other information relating to personal data that has been or is being processed by them.

According to the PDPA, where processing is carried out on behalf of a Data User, the Data User shall ensure that the Data Processor provides enough guarantees in respect of the technical and organisational security measures governing the processing to be carried out and takes reasonable steps to ensure compliance with these measures. In particular, the Regulations of 2013 require the Data User to comply with the security standards set out by the Commissioner, and ensure that such standards are complied with by any Data Processor that processes data on its behalf.

The Personal Data Protection Commissioner also released two circulars in February 2022. Those circulars are meant to remind prescribed classes of Data Users of their obligation under the PDPA to register with the PDPD and to renew their certificates of registration before expiry.

A list of the 13 prescribed classes of Data Users can be found in the circulars.

⁴ Personal Data Protection Commissioner Circular No. 1/2022: Requirement to Register as Data User under the Personal Data Protection Act 2010 (Act 709). Personal Data Protection Commissioner Circular No. 3/2022: Obligation to Renew Certificate of Registration as Data User under the Personal Data Protection Act 2010 (Act 709)

Both the GDPR and the PDPA define the roles of Data Controllers (Data Users in the PDPA) and Data Processors according to the control they exercise in the processing of data.

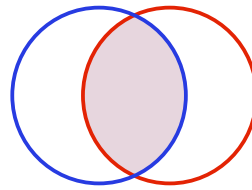
In the GDPR, the Data Controller qualification is triggered by the decision of the goals and methods of the processing. In the PDPA, a Data User is the person who processes personal data for its own purposes or has control over the processing of the data or authorises it.

Both the GDPR and the PDPA define the Data Processor as the person who processes data on behalf of a controller. The PDPA states specifically that a Data Processor does not process data for any of its own purposes. The PDPA is less detailed than the GDPR about the definition of roles between the controller and the processor, for example, it does not establish any rules about the erasure of data. However, similar to the GDPR, the PDPA regulates the definition of roles between the Data User and the Data Processor in terms of security standards. The Regulations of 2013 require the Data User to comply with security standards adopted by the Commissioner and to ensure the compliance of its Data Processors with these security standards.

One of the Proposed Amendments of the Communications and Multimedia Minister ("Minister") is to impose on Data Processors the obligation to adhere to the PDPA's security principle.

Lawfulness

Criterion 6. Legal Bases



60%

Fairly Similar

GDPR

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.

Section 6

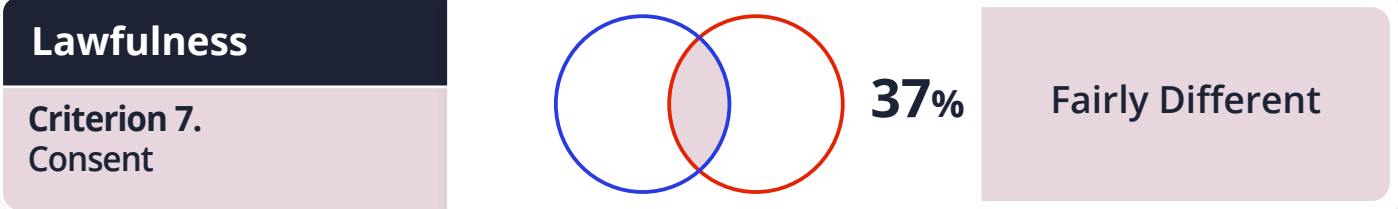
PDPA

Data Users are required to obtain consent from the Data Subject except when the processing is necessary for the following purposes:


- The performance of a contract entered into with a Data Subject.
- For taking steps at the request of the Data Subject with a view to entering into a contract.
- In order to comply with any legal obligation that the Data User is subject to.
- In order to protect the vital interests of the Data Subject.
- For the administration of justice.
- For the exercise of any functions conferred upon any person by the law.

Consent is the cornerstone of the PDPA, while the GDPR treats consent in the same way as the other legal bases. Both the GDPR and the PDPA include processing that is necessary to the performance of a contract, including pre-contractual requirements, compliance with legal obligations, and the protection of vital interests of the Data Subject. The PDPA provides two legal bases for the administration of justice and for the exercise of any function conferred upon any person by the law. These two legal bases are included in a wider legal basis in the GDPR: the legal basis for processing 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.

Finally, the GDPR provides a legal basis for the legitimate interests of the Data Controller or a third party, and the PDPA does not provide any such legal basis.



 **GDPR** Articles 4(11), 7, Recitals 32, 42, 43

Sections 7, 38  **PDPA**

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”.

The PDPA does not specify how the consent must be collected. However, consent is part of the “notice and choice” principle, which focuses entirely on the notice. We can conclude that the PDPA requires the consent to be at least informed.

The PDPA also provides the Data Subject with the right to withdraw their consent to the processing of personal data in writing.

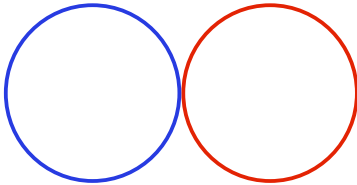
Regulations of 2013, Section 3

The 2013 regulation establishes a set of criteria for gaining valid consent:

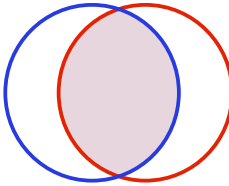
- The requirement to obtain consent shall be presented as distinguishable in its appearance from other matters.
- The obtaining of consent must be demonstrable by the Data User: it must be recorded or maintained, and the burden of proof lies on the Data User.

The GDPR is very demanding in terms of quality of consent: it must be an informed, freely given, specific, and unambiguous indication of the Data Subject’s wishes, provided through a statement or a clear affirmative action. In addition, the consent can be easily withdrawn at any moment, without prejudice to the Data Subject. The PDPA provides none of these requirements, except for the fact that the PDPA requires the Data User to supply a privacy notice to the Data Subject, and that the Data Subject is entitled to withdraw their consent.

Both the GDPR and the PDPA require the consent to be demonstrable. In the GDPR, the Data Controller is required to be able to prove a valid consent (with all the required qualities). In the PDPA, the Data User is required to prove that the consent has been collected, that the requirement to obtain consent was distinguishable in its appearance from other matters, and that the privacy notice has been communicated.

Lawfulness	 <p>0%</p>	Different
Criterion 8. Legitimate Interest		

Contrary to the GDPR, the PDPA does not provide a legal basis for legitimate interests.

Lawfulness	 <p>70%</p>	Fairly Similar
Criterion 9. Conditions for the Processing of Sensitive Data		

 **GDPR**

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

Section 26

PDPA 

The processing of sensitive personal data is forbidden, except for the following eight legal bases:

1. Explicit consent.
2. Complying with right or obligation conferred or imposed by law in the employment consent.
3. The protection of the vital interests of the Data Subject or third party if consent cannot be given or reasonably be expected.
4. Medical purposes undertaken by a healthcare professional or a person who, in the circumstances, owes a duty of confidentiality which is equivalent to that which would arise if that person were a healthcare professional.
5. Legal purposes: for the purposes of, or in connection with, any legal proceedings; for the purposes of obtaining legal advice; for the purposes of establishing, exercising, or defending legal rights; for the administration of justice.
6. The exercise of any functions conferred on any person by or under any written law.
7. Information made public as a result of steps deliberately taken by the Data Subject.
8. Any other purposes as the Minister sees fit.

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.

Both the GDPR and the PDPA provide a principle of prohibition of processing sensitive data except where the processing is based on legal bases specific to sensitive data. The GDPR and the PDPA are similar in the definition on these legal bases, as both allow the processing of sensitive data on the basis of:

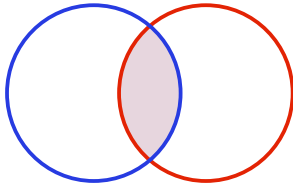
- Explicit consent.
- Rights conferred and obligations imposed by law in the context of employment.
- The protection of vital interest of the Data Subject or another person when consent cannot be given by the Data Subject.
- The establishment, exercise, or defence in legal claims and other judicial-related purposes.
- The fact that the data have been made public by the Data Subject (manifestly for the GDPR, deliberately for the PDPA).
- Medical purposes.

Both the GDPR and the PDPA provide a legal basis for public organisations, but the GDPR's legal basis is narrower because it must be proved that the processing is necessary for reasons of substantial public interest or public interest in the area of public health.

Contrary to the GDPR, the PDPA does not provide a legal basis for archiving, scientific, or historical research purposes. However, under PDPA, the Minister has been given the power to provide additional legal bases, whereas the GDPR does not include such a provision.

Lawfulness

Criterion 10. Children



35%

Fairly Different

GDPR

**Articles 6, 8, 12, 40, 57,
Recitals 38, 58, 75**

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.

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.

When children's personal data is used for marketing or gathered for information society services presented directly to children, special protection should be provided.

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.

In the case of information society services, the GDPR's requirements on the appropriate circumstances for processing children's data apply.

Section 4

PDPA

If the Data Subject is under 18 years of age, the PDPA defines the relevant person with respect to a Data Subject as "the parent, guardian, or person with parental responsibility on behalf of the Data Subject".

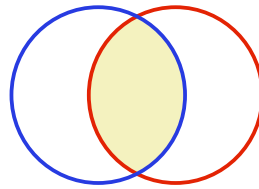
Regulations of 2013, Section 3

If the Data Subject is under the age of 18 years, the Data User must obtain consent from the parent, guardian, or person who has parental responsibility over the Data Subject.

In both the GDPR and the PDPA, the consent of the parents, guardian or person who has parental responsibility for the minor is necessary to process their data. However, in the PDPA, individuals under 18 are considered minors, whereas in the GDPR, the age of 16 is stated, and a certain freedom is left to EU Member States, which may lower it to 13. The GDPR additionally provides transparency requirements specifically appropriate for children.

Data Subjects' Rights

**Criterion 11.
Transparency Requirements**




55%

Fairly Similar

GDPR Article 12, Recital 58

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”.

The information to be provided is precisely detailed in the GDPR.

Section 7. Regulations of 2013, Section 4 **PDPA** 

According to the Notice and Choice Principle, the Data User must communicate to the Data Subject a written notice to inform them about the processing where it is based on consent. The PDPA specifies that such a notice must be in the national and English languages. In addition, the individual is provided with a clear and readily accessible means to exercise their choice.

The information that must be provided is precisely detailed in the PDPA and the Regulations of 2013.

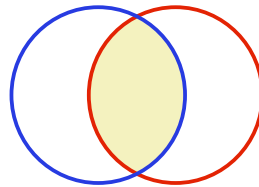
The GDPR and the PDPA are different in their approach to the information required to be communicated to the Data Subject. On the one hand, the GDPR provides a general transparency requirement that applies regardless of the legal basis of the processing. On the other hand, the PDPA provides a “notice and choice principle” that only applies when the processing is based on consent.

The requirements attached to how the information must be communicated to the Data Subject also differ. The PDPA specifies that the information must be in the national and English language, and provided with a clear and readily accessible means for the Data Subject to exercise their choice. The GDPR requires information to be easy to understand for the Data Subject, concise, easily accessible, and delivered using clear and simple language.

Both the GDPR and the PDPA provide specific categories of information to communicate to the Data Subject.

Data Subjects' Rights

Criterion 12. Right of Access



55%

Fairly Similar

GDPR

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.

Sections 12, 30-32

PDPA

Data Subjects have the right to access their personal data held by a Data User.

In their request, the Data Subject asks for information that is processed by or on behalf of the Data User and the communication of a copy of their personal data in an intelligible form. The Data Subject makes a separate data access request for each purpose.

According to the PDPA, the Data User is entitled to reject data access requests where the Data User may ask for more information for verification purposes, where the request would represent an excessive burden or expense for the Data User, or where the right of access would infringe other persons' rights and freedoms.

The Data Subject must comply with a data access request or communicate its rejection of the data access to the Data User no later than 21 days from the date of receipt of the data access request.

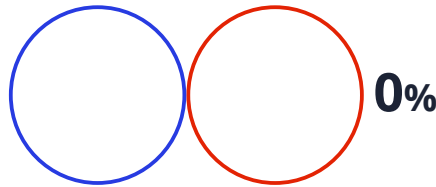
The right to access is subject to the payment of a prescribed fee.

Both the GDPR and the PDPA provide Data Subjects with the right to access their personal data when it has been collected and processed by a Data Controller.

However, the laws have several differences with regard to the implementation of the right of access. The data access request is free of charge in the GDPR and includes any data collected or processed by the Data Controller and its processor, whereas it is subject to a fee and specific to a purpose in the PDPA. There are also differences in terms of the deadline for the Data Controller to respond and in terms of limitations of the right of access.

Data Subjects' Rights

Criterion 13.
Right to Data Portability



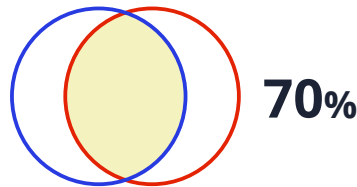
Different

Contrary to the GDPR, the PDPA does not provide a right to data portability.

However, the Communications and Multimedia Minister ("Minister"), who supervises the implementation of the PDPA, has indicated that various proposed adjustments to the PDPA would be submitted to Parliament for approval in October 2022. Among those proposed amendments seems to be an introduction of data portability. A new provision will be introduced in the amendment bill to grant Data Subjects the right to data portability under the PDPA.

Data Subjects' Rights

Criterion 14.
Right to Rectification



Fairly Similar

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.

The PDPA grants Data Subjects the right to make a data correction request in order for the Data User to correct inaccurate, incomplete, misleading, or not up-to-date data.

If the personal data has been disclosed to a third party during the 12 months immediately preceding the day on which the correction is made, the Data User must take all practical steps to supply the third party with a copy of the corrected personal data accompanied by a notice in writing stating the reasons for the correction.

Both the GDPR and the PDPA grant Data Subjects the right to ask for correction of their inaccurate personal data. In the GDPR, the Data Controller must communicate the corrected data to each recipient to which it was disclosed, unless this would involve a disproportionate effort, whereas in the PDPA, the same obligation only applies to the Data Controller if the data has been disclosed during the 12 months preceding the day on which the correction is made.

GDPR

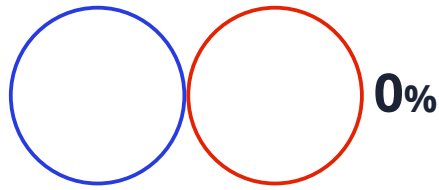
Article 16

Sections 34, 35

PDPA

Data Subjects' Rights

Criterion 15.
Right to be Forgotten /
Right to Erasure

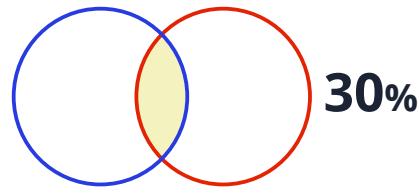


Different

Contrary to the GDPR, the PDPA does not provide any right to erasure.

Data Subjects' Rights

Criterion 16. Right to Object



Fairly Different

GDPR **Article 21**

Data Subjects have the right to object to the processing of their personal data if:

- 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.

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.

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.

Sections 42, 43 **PDPA**

Data Subjects have the right to object to the processing of their personal data when the processing is likely to cause damage or distress, except if the processing:

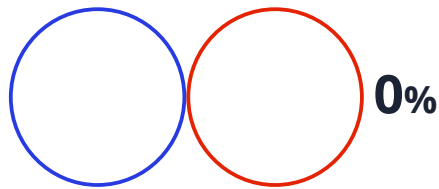
- Is based on the consent of the Data Subject.
- Is necessary for the performance of a contract to which the Data Subject is a party (including steps with a view to entering a contract).
- Is necessary for compliance with legal obligations to which the Data User is the subject.
- Is necessary in order to protect the vital interests of the Data Subject.

Data Subjects can also object to the processing of their personal data for the purposes of direct marketing by a notice in writing.

Both the PDPA and the GDPR provide a right to oppose processing for purposes of direct marketing. In the PDPA, it is called “the right to prevent processing for purposes of direct marketing”.

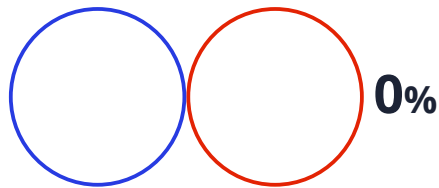
Contrary to the PDPA, the GDPR provides, under certain conditions, the right to oppose: processing based on the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller; processing based on the legitimate interest of the Data Controller or third parties; and processing of personal data for scientific, historical research, or statistical purposes unless the processing is necessary for the performance of a task of public interest.

Contrary to the GDPR, the PDPA provides, under certain conditions, the right to object to the processing of their personal data when the processing is likely to cause damage or distress.

Data Subjects' Rights**Criterion 17.**
Rights Related to Profiling

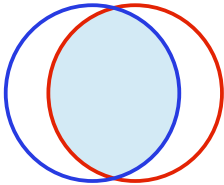
Different


Rights related to profiling are explicitly contained in the GDPR. Such rights do not seem to contain equivalent in Malaysian law.

Data Subjects' Rights**Criterion 18.**
Right to Restrict the Use of
the Personal Data


Different

The right to restrict the use of personal data is explicitly contained in the GDPR. This right does not seem to contain an equivalent in Malaysian law.

<p>Accountability Requirements</p> <p>Criterion 19. Appointment of a Representative</p>	 <p>75%</p>	<p>Similar</p>
---	---	-----------------------

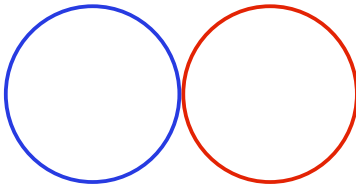
 **GDPR** **Article 27, Recital 80**

Data Controllers and Data Processors not established in the EU (but that are subject to the GDPR) must appoint a representative in the EU, except if processing is occasional and does not involve large-scale processing of sensitive data.

Section 2 **PDPA** 

If a Data User is not established in Malaysia but is subject to the PDPA, the Data User must nominate a representative established in Malaysia for the purposes of the PDPA.

Both the GDPR and the PDPA require Data Controllers to appoint a representative in their territory when a Data Controller is subject to their provisions but is not established in their territory.

<p>Accountability Requirements</p> <p>Criterion 20. Appointment of a DPO</p>	 <p>0%</p>	<p>Different</p>
--	--	-------------------------

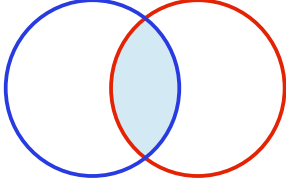
Contrary to the GDPR, the PDPA does not require Data Users to appoint a Data Protection Officer (DPO).

Data users are not required under the PDPA to designate DPO at this time. In accordance with the Public Consultation Paper, the Commissioner has recommended mandating that Data Users appoint DPOs, as well as publishing criteria for the appointment of DPOs (e.g., the categories of Data Users that are required to appoint DPOs).

Recent indications from JPDP (Malaysian Department of Personal Data Protection) suggest that the amended bill would likely require Data Users to designate at least one DPO for their organisation.

Accountability Requirements

Criterion 21.
Record of Processing



40%

Fairly Different

GDPR

Article 30, Recital 82

Data Controllers and Data Processors are required to keep a record of processing actions under their control. Furthermore, the GDPR establishes a list of data that a Data Controller must keep track of:

- The Data Controller’s name and contact information.
- The purposes of the processing.
- A description of the categories of personal data.
- The categories of recipients to whom the personal data will be disclosed.
- The estimated time for erasure of the categories of data.
- A general description of the technical and organisational security measures used.

The GDPR also establishes a similar list for Data Processors, mandates that records be kept in writing or electronically, and specifies exceptions for businesses with fewer than 250 employees, unless the processing is likely to jeopardise Data Subjects’ rights and freedoms, is not routine, or involves special categories of data.

Section 44

PDPA

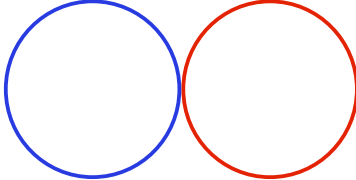
Data Users are required to keep and maintain a record of any application, notice, request or any other information relating to personal data that has been or is being processed by them.

Both the GDPR and the PDPA require Data Controllers and Data Processors to keep a record of processing actions that have been exercised under their control.

However, these record differ. On one hand, the GDPR requires controllers to keep a record of how the personal data is processed in its organisation. On the other hand, the PDPA requires the Data Users to keep a record of any legal event relating to personal data processed by them. In practice, Data Controllers subject to the GDPR will also have to keep these records as part of their obligation to demonstrate their compliance.

Accountability Requirements

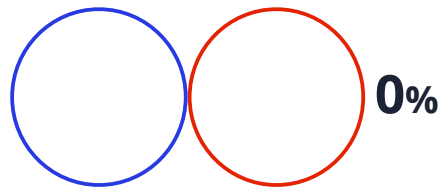
Criterion 22.
Data Protection Impact Assessment (DPIA)



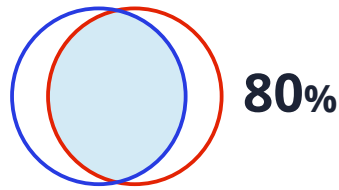
0%

Different

Contrary to the GDPR, the PDPA does not require Data Users to conduct a Data Protection Impact Assessment (DPIA).

Accountability Requirements**Criterion 23.**
Privacy by Design**Different**

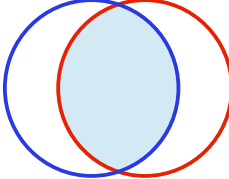
Contrary to the GDPR, the PDPA does not provide any privacy by design principle.

Accountability Requirements**Criterion 24.**
Audit Requirements**Similar**

Neither the GDPR nor the PDPA require Data Controllers to conduct audits. However, the GDPR mentions audit as a way to demonstrate compliance.

Accountability Requirements

Criterion 25. Appointment of Processors



70%

Fairly Similar

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.

Section 9

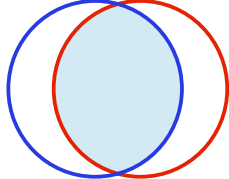
PDPA

Where processing of personal data is carried out by a Data Processor on behalf of the Data User, the Data User shall ensure that the Data Processor provides sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out and takes reasonable steps to ensure compliance with those measures.

Personal Data Protection Standard 2015

The Data User shall bind the appointed party with a contract for operating and carrying out personal data processing activities.

Both the GDPR and the PDPA require the Data Controllers to appoint, through a binding agreement, Data Processors that provide sufficient guarantees, either in terms of security measures (PDPA) or in terms of the application of all the provisions of the Regulation (GDPR).

Accountability Requirements Criterion 26. Information Security		68%	Fairly Similar
---	---	------------	-----------------------


GDPR
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.

Section 9

PDPA 

Data Users are required to take practical steps to protect the personal data from any loss, misuse, unauthorised or accidental access or disclosure, alteration, or destruction, by having regard to:

- The nature of the personal data and the harm that would result from such security failures.
- The place or location where the personal data is stored.
- Any security measures incorporated into any equipment in which the personal data is stored.
- The measures taken for ensuring the reliability, integrity, and competence of personnel that have access to the personal data.
- The measures taken for ensuring the secure transfer of the personal data.

Personal Data Regulations of 2013, Section 6

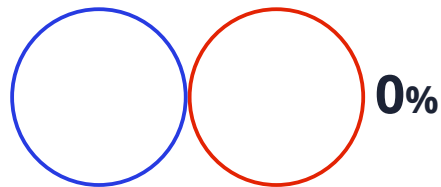
Data Users are required to:

- Develop and implement a security policy.
- Ensure that the security policy and the Data Processors comply with the security standards set out by the Commissioner (last security standards were adopted in 2015).

The GDPR requires Data Controllers and Data Processors to ensure adequate security in the processing of personal data, taking into account the nature of the personal data collected and the harm that would result from a security breach of the processing. Data Controllers and Data Processors also have to take into account the state of the art of security measures and the cost of their implementation.

Contrary to the GDPR, Malaysia’s Personal Data Regulations of 2013 only require Data Controllers to implement security standards set out by the Commissioner. Under the existing PDPA, Data Processors are not directly required to comply with the law's provisions, it is the Data Users who are responsible for any noncompliance by Data Processors with any PDPA requirements.

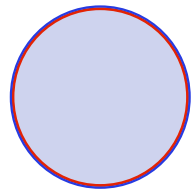
In response to the Public Consultation Paper and the rising frequency of data breach events involving Data Processors, the Commissioner has suggested adding measures to the PDPA to regulate Data Processors directly. Specifically, the JPDP has just verified that the proposed amendment bill would place a direct requirement on Data Processors to comply with the security principle outlined in Section 9 of the PDPA.

Accountability Requirements**Criterion 27.
Breach Notification****Different**

Contrary to the GDPR, the PDPA does not require Data users to notify data breaches to the Commissioner and Data Subjects. Currently, Data Users are notifying the Commissioner of data breaches on a voluntary basis, if at all.

JPDP has recently confirmed that a mandatory data breach notification regime will be included in the amendment bill, and that Data Users will be required to report data breach incidents to the Commissioner within 72 hours of discovering the incident, using the Commissioner-provided template data breach notification form. JPDP did not give more information on the parameters and criteria for making such a notice (e.g., number of affected data subjects, whether only confirmed data breach incidents meeting a certain threshold must be notified to the Commissioner, etc.).

Data Localisation and Transfer
Criterion 28.
Data Localisation Requirements

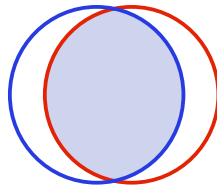


100%

Similar

Neither the GDPR nor the PDPA provide any data localisation requirements.

Data Localisation and Transfer
Criterion 29.
International Data Transfer



78%

Similar

1 2

 **GDPR** **Articles 5, 44-50**

Section 129 **PDPA** 

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.

The PDPA provides a general prohibition of transfer of personal data to a place outside of Malaysia, unless the Minister has specified the place upon the recommendation of the Commissioner (countries whose regulation is substantially similar to the PDPA, or that follows the same purposes, or a place that ensures an adequate level of protection at least equivalent to the level of protection of the PDPA).

If a place has not been specified by the Minister, a Data User may transfer any personal data to a place outside Malaysia if:

- The Data Subject has given their consent to the transfer.
- The transfer is necessary for the performance of a contract between the Data Subject and the Data User.
- The transfer is necessary for the performance of a contract between a Data User and a third party which has been entered into at the request of the Data Subject or is in the interest of the Data Subject.
- The transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights.
- The Data User has reasonable grounds for believing that in all circumstances of the case, the transfer is for the avoidance or mitigation of adverse action

- 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.

against the Data Subject, it is not practicable to obtain the consent in writing from the Data Subject to that transfer, and if it was practicable to obtain such consent, the Data Subject would have given their consent.

- The Data User has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not be processed in that place in any manner which, if that place were Malaysia, would be a contravention of the PDPA.
- The transfer is necessary in order to protect the vital interests of the Data Subject.
- The transfer is necessary as being in the public interest in circumstances as determined by the Minister.

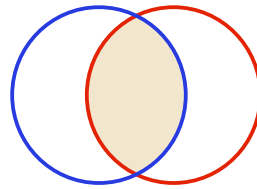
Both the GDPR and the PDPA provide a general prohibition of international data transfers, unless a provision authorises the transfer. In both the GDPR and the PDPA, the preferable procedure to transfer personal data is the assessment of the adequate level of protection of the third country by the competent authority (the European Commission for the GDPR, the Ministry for the PDPA).

The GDPR also allows transfers that are based on adequate safeguards (including binding corporate rules and Standard Contractual Clauses). The PDPA does not provide the concept of “adequate safeguards” but allows transfers in a similar way when the Data User has taken “all reasonable precautions” and exercised “all due diligence” to protect personal data in the third country in the same way that it would have been protected in Malaysian.

Both the GDPR and the PDPA also provide special legal bases for transfers that are not based on the assessment of the adequate level of protection (and on the appropriate safeguards for the GDPR). The legal bases differ, but some are similar such as consent, the performance of a contract between the Data User and the Data Subject or between the Data User and a third party in the interest of the Data Subject, and the protection of vital interests.

Enforcement

Criterion 30. Data Protection Authority



57%

Fairly Similar

GDPR

Articles 31, 51-59

The supervisory authorities have the jurisdiction to:

- 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.

In accordance with EU or Member State procedural law, the supervisory authorities have the authority to:

- 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.

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.

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.

The GDPR explicitly states that each supervisory authority must carry out its responsibilities and wield its powers independently.

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.

Sections 47-69, 83-109

PDPA

The Commissioner is appointed by the Minister. The Minister was appointed the Department of Personal Data Protection on May 16th 2011.

The Commissioner has in particular, the following functions:

- To implement and enforce the personal data protection laws, including the formulation of operational policies and procedures.
- To monitor and supervise compliance with the provisions of the PDPA, including the issuance of circulars, enforcement notices and any other instruments.

After receiving a complaint, the Commissioner has the jurisdiction to carry out an investigation in relation to a Data User to ascertain whether the Data User contravenes the provisions of the PDPA.

The PDPA also established an appeal tribunal for the purpose of reviewing appeals from persons aggrieved by a decision of the Commissioner.

The Commissioner is under the Minister's direction as they respond to the Minister and are obligated to give effect to the Minister's directions of general character relating to the performance of the Commissioner's functions and powers. The Commissioner also has an obligation to inform the Minister about their activities and finances.

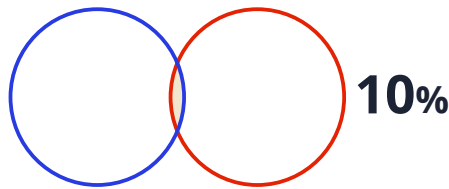
The Commissioner is funded by the Personal Data Protection Fund, which includes in particular sums provided by the Parliament, fees, costs and charges imposed by or payable to the Commissioner, and sums derived from financial dealings with the Commissioner (sales, disposal, lease etc.).

Both the GDPR and the PDPA provide supervisory authorities powers to enforce the data protection laws applicable to the territory in which they have jurisdiction. In particular, both the GDPR and PDPA provide supervisory authorities the jurisdiction to carry out investigations and to issue sanctions.

Contrary to the GDPR, which expressly states that each supervisory authority carries out its powers independently, the PDPA clearly states that the Commissioner carries out its function under the Minister's direction. In addition, the PDPA establishes a special fund for the Commissioner, whereas the GDPR is silent on the source of funding available to regulatory bodies.

Enforcement

Criterion 31. Penalties



Different

GDPR 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.

Sections 5, 16, 18, 19, 29, 37, 38, 40, 42, 43, 130 **PDPA**

The Data User is liable to a fine not exceeding RM 500,000 (approximately €108,000) when:

- The Data User collects personal data in an unlawful way (in particular without the consent of the Data Subject).
- The Data User is subject to the obligation to obtain a certificate of registration from the Commissioner and contravenes this registration requirement (by not registering or by processing data after its revocation).

The Data User is liable to a fine not exceeding RM 300,000 (approximately €65,000) when:

- The Data User contravenes the personal data protection principles.
- The Data User fails to comply with the provisions relating to the processing of sensitive data.
- The Data User fails to comply with third-country transfer requirements.

The Data User is liable to a fine not exceeding RM 200,000 (approximately €43,000) when:

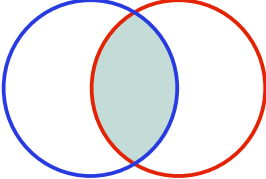
- The Data User fails to comply with the opposition of the Data Subject to a processing that could cause harm.
- The Data User fails to comply with the opposition of the Data Subject to processing for the purposes of direct marketing.
- The Data User fails to surrender its certificate to the Commissioner within seven days after its revocation.



The Data User is liable to a fine not exceeding RM 100,000 (approximately €21,500) when:

- The Data User fails to comply with a data correction request.
- The Data User fails to comply with the withdrawal of consent of the Data Subject.
- The Data User is subject to a Code of Practice and fails to comply with it.

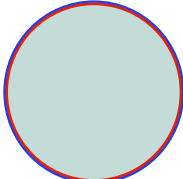
The PDPA specifically defines the different maximum amounts for fines that can be imposed by the Commissioner. The fines go up to RM 500,000.

In the GDPR, the supervisory authority can impose fines up to €20 million and 4% of global annual turnover, which is more dissuasive as the fine can be adapted to the size of the company.

<p>Exemptions</p> <p>Criterion 32. Anonymised Data</p>	 <p>50%</p>	<p>Fairly Similar</p>
--	---	-----------------------

<p> GDPR</p> <p>Recital 26</p>	<p>Section 4</p> <p>PDPA </p>
<p>The GDPR does not apply to data that has been "anonymised", meaning that it can no longer be used to identify the Data Subject.</p>	<p>There is no mention of the applicability of the law to anonymised data. However, the PDPA defines personal data as data relating directly or indirectly to a Data Subject, who is directly or indirectly identified or identifiable from that information.</p>

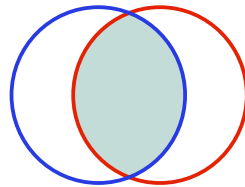
The GDPR expressly excludes anonymised data from the scope of its provisions. The PDPA does not expressly exclude anonymised data, but its definition of personal data can be interpreted as a tacit exclusion of anonymised data.

<p>Exemptions</p> <p>Criterion 33. Social Media Intermediaries and Identity Management</p>	 <p>100%</p>	<p>Similar</p>
--	--	----------------

Neither the GDPR nor the PDPA mention social media intermediaries and identity management.

Exemptions

Criterion 34. Exemptions for Research



65%

Fairly Similar



Articles 5, 9, 14, 17, 89
Recitals 33, 156, 159-161

Personal data processing for research purposes is governed by specific standards under the GDPR.

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”.

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.

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.

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.

Section 45



The PDPA provides a special exemption relating to processing with research purposes.

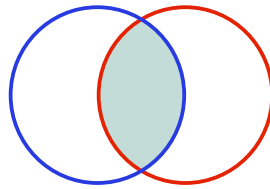
Processing can be exempted from the general principle, the notice and choice principle, the disclosure principle, the access principle and other related provisions in the PDPA if:

- The personal data is processed for preparing statistics or carrying out research and is not processed for any other purpose.
- The resulting statistics or the results of the research are not made available in a form which identifies the Data Subject.

Both the GDPR and the PDPA provide exemptions to their provisions that are specific to the purpose of research. However, the scope of the exemptions differ. In the PDPA, the exemption applies as soon as the processing is only for research purposes and the results are not made available in a form which identifies the Data Subject. In the GDPR, the exemptions are more complex and focus on the necessity of such restrictions for the purposes of the processing.

Exemptions

Criterion 35.
Application to Public Authorities



50%

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.

Sections 2, 3

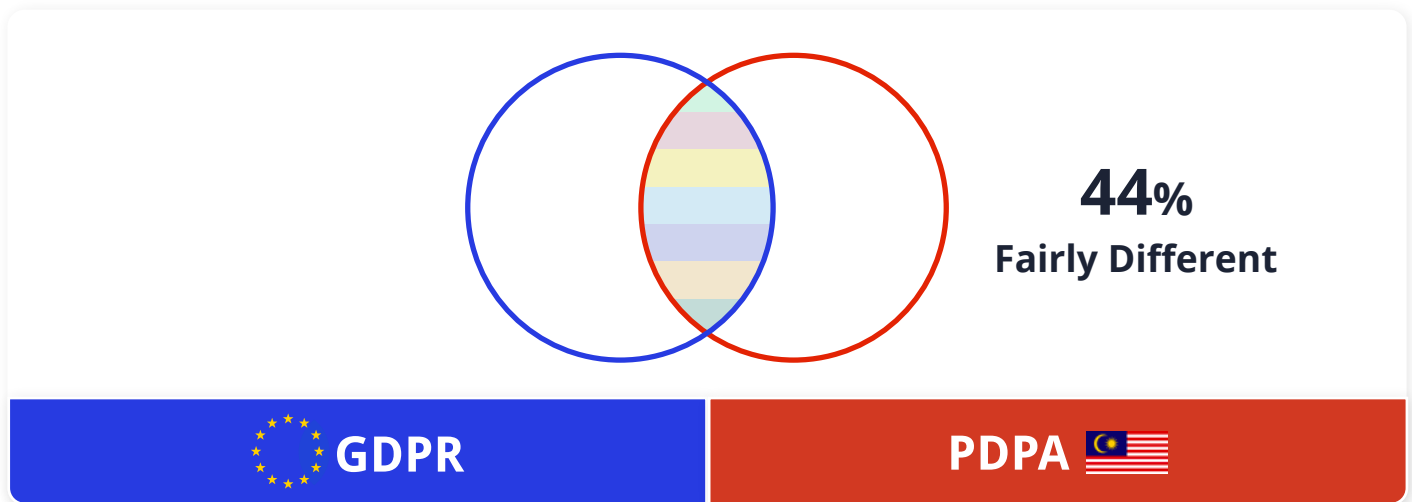
PDPA 

The PDPA is not applicable to the Federal Government and State Governments. In addition, as the PDPA only applies in the context of processing in respect of commercial transactions, the PDPA would be applicable to public authorities only when they engage in such activities.

The GDPR has a wider scope than the PDPA as it applies to public authorities when the proceedings are not in connection with their official tasks, whereas the PDPA is applicable to such authorities only when they engage in commercial transactions (and is not applicable to the Federal Government and State Governments).


In light of growing reports of data breach incidents involving the government, the JPDP has indicated that the amendment bill will extend the application of the PDPA to require both the Federal and State governments to comply with the PDPA's requirements when conducting personal data processing activities. JPDP has also emphasised that, should this plan be enacted, JPDP would need to be an independent body in order to carry out its regulatory responsibilities under the PDPA successfully.

Conclusion



The PDPA and the GDPR are fairly different. Therefore, doing business in the EU and in Malaysia requires an important privacy gap analysis effort for companies.

However, the Review of the Personal Data Protection Act, currently under public consultation, is likely to approximate the PDPA and the GDPR. The table below summarises some of the suggested improvements disclosed by Public Consultation Paper No. 01/2020.

Criterion	Suggested improvement	Similarity 
Criterion 1. The Territorial Scope	Application of the PDPA to Data Users outside Malaysia which monitor Malaysian data.	↑
Criterion 2. The Subject Matter Scope	Considering excluding business contact information from the PDPA.	↓
	Considering including the processing of personal data in non-commercial transactions.	↑
Criterion 5. Relevant Parties	Explicit applicability of PDPA for Data Processors.	↑
Criterion 7. Consent	Add clarity for consent provision, may include the consent to be specific.	↑
Criterion 12. Right of Access	Requirement to inform the Data Subject of the third party to which their data have been/to be disclosed.	↑
Criterion 13. Right to Data Portability	Insertion of a new provision on the right to data portability.	↑

Criterion 16. Right to Object	<p>Establishment of a do-not-call registry to opt-out from receiving unsolicited direct marketing materials.</p> <p>Guidance on the way to provide a clear mechanism for Data Subject to unsubscribe from online services, and for the opt-out method for direct marketing calls.</p>	<p>=</p>
Criterion 20. Appointment of a DPO	<p>Requirement to appoint a DPO to oversee data protection strategy and increase the level of compliance.</p>	<p>↑</p>
Criterion 23. Privacy by Design	<p>Requirement for any new system to apply privacy by design (for all Data Users).</p>	<p>↑</p>
Criterion 27. Breach Notification	<p>Data breach notification to the Commissioner.</p>	<p>↑</p>
Criterion 29. International Data Transfers	<p>Removal of the whitelist issued by the Minister and additional security requirements.</p>	<p>↓</p>
Criterion 35. Application to Public Authorities	<p>Extension of the scope of the PDPA to Federal Government and State governments.</p>	<p>↑</p>

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:

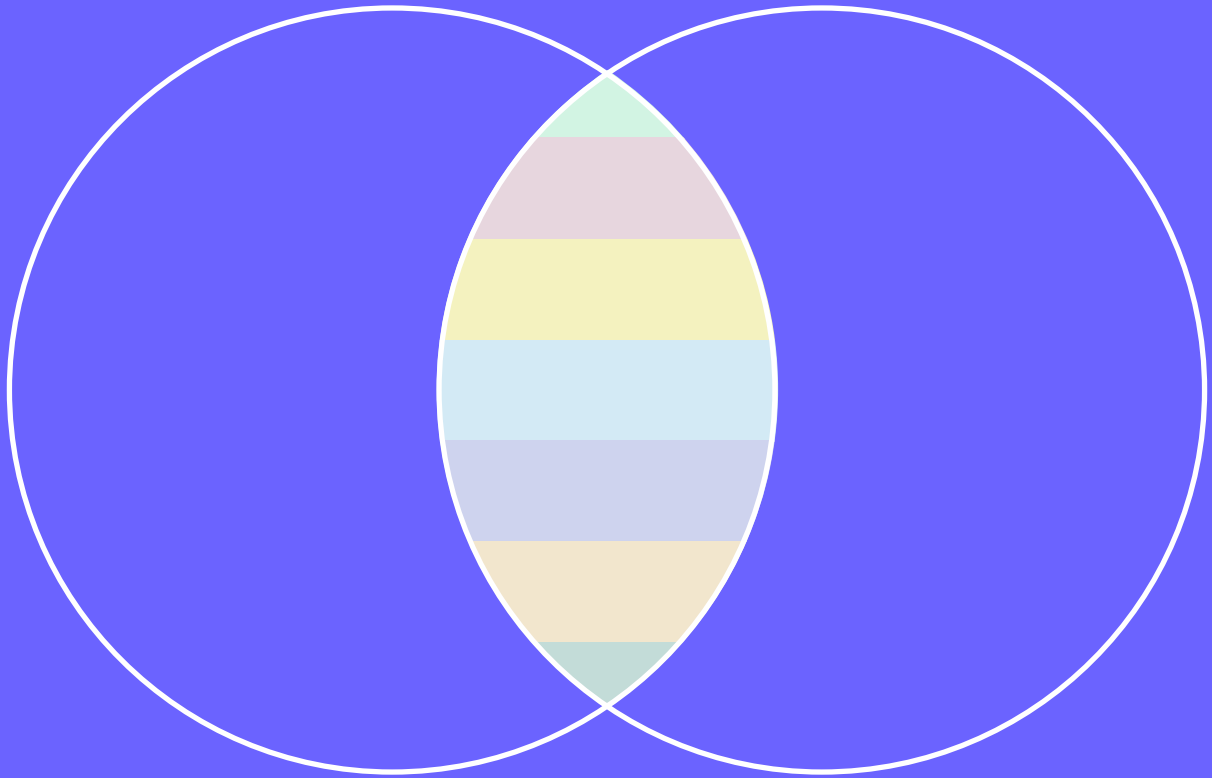
✓ Detect

✓ 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