Luther.

# Data Protection in Malaysia for EU Companies

## August 2024 update



unyer GLOBAL ADVISORS

# Content

**A. Introduction** 3

**B. Personal Data** 4

**I. General Compliance** ..... **4**
1. Malaysia: the PDPA ..... 4
2. The EU: the GDPR ..... 6
3. Key differences between the PDPA and the GDPR ..... 8

**II. Cross-border data transfers** ..... **10**
1. Transfers from Malaysia to the EU ..... 10
2. Transfers from the EU to Malaysia ..... 10

**C. Use and Regulation of Data** 11

**I. Data Act** ..... **11**
1. Background ..... 11
2. Key provisions ..... 11
3. Key objectives ..... 12
4. Impact on businesses ..... 12
5. Impact in Malaysia ..... 13

**II. Data Governance Act** ..... **13**
1. Background ..... 13
2. Key Provisions ..... 13

**III. Cybersecurity Legislation** ..... **14**

**D. Artificial Intelligence** 15

**I. EU AI Act** ..... **15**

**II. Impact in Malaysia** ..... **16**
1. Impact on the legal landscape ..... 16
2. Impact on Malaysian businesses ..... 16

**E. Your contact persons** 17

**Hits the mark. Luther.** 18

**About unyer** 18

**Our locations** 19

**Our awards** 20

# A. Introduction

In an increasingly digital and connected world, data has become a dominant force. The rise of big data has become a reality, and with it comes an increase in regulations surrounding topics such as personal data, cybersecurity, or artificial intelligence. As a result, it is essential for organisations to understand not only where data is relevant, but also how and where it is transferred. Indeed, with cross-border data flows becoming more commonplace every day, even if an organisation has complied with all its local obligations, it now needs to consider what will happen should its data crosses borders.

For European Union (**"EU"**) companies operating either directly or through group companies in Malaysia, it is essential to understand both Malaysian data-related laws and how their EU obligations extend to their operations in Malaysia. For example, any transfer of personal data between EU-based companies and their subsidiaries in Malaysia will be a cross-border transfer and both companies will need to comply with their respective obligations.

In Malaysia, the Personal Data Protection Act 2010 provides the legal framework for the collection, use and disclosure of personal data, while in the EU, this role is fulfilled by the General Data Protection Regulation. For its part, the EU has recently adopted new wide-ranging legislation to address data sharing and fair access to and use of data in the era of cloud computing and the so-called "Internet of Things" ("**IoT**").

As concerns around the use of data grow, reforms are being discussed and new legislation is being implemented around the world. It is therefore imperative that companies keep up to date with local legislation and the resulting obligations.

This brochure aims to provide EU companies with an overview of their legal obligations and the requirements for doing business in Malaysia in relation to both the protection of personal data (Part B) and the use of data in general under both Malaysian and EU law (Part C).

In addition, as artificial intelligence (**"AI"**) has become increasingly important in our daily lives, from virtual assistants to self-driving cars, the manner in which AI uses data has also become a growing concern. The EU has recently taken an important step towards establishing a regulatory framework to ensure that the development and use of AI in the EU is safe, ethical and respects fundamental rights, with the introduction of the EU AI Act, which is sparking discussion across jurisdictions (Part D).

# B. Personal Data

Protection of personal data has become a critical issue across the globe. The proliferation of digital devices and data use, the ease of data transfers and the increasing prevalence of cyber-attacks have increased the risk of data breaches and misuse of personal information. As a result, it is more important than ever for organisations to safeguard their data: one key aspect of this is ensuring that they are compliant with local data protection laws. In addition, EU companies operating in Malaysia should be aware of the key differences between EU and Malaysian law and take care to ensure compliance when transferring personal data across borders.

## I. General Compliance

Personal data is defined as any information relating directly or indirectly to a natural person who is identified or identifiable from that data. Nowadays, virtually all companies process personal data, even if it is only that of their employees, and are therefore directly affected by personal data protection legislation. EU-based companies who operate in Malaysia, in particular, will have a range of obligations in terms of personal data protection ("**PDP**") and, depending on the circumstances, they may need to comply with Malaysian law, EU law, or both, particularly if they ever transfer personal data.

### 1. Malaysia: the PDPA

Malaysia enacted the Personal Data Protection Act 2010 (**"PDPA"**), which came into force on 15 November 2013, to regulate the processing of personal data, which has been complemented by various regulations, standards, and codes of practice.

There have been many calls in Malaysia in recent years for amendments to the PDPA to strengthen both the law and its enforcement. Following a consultation paper in 2020, an amendment bill was drafted in 2022 and finally tabled in 2024. In July 2024, the Personal Data Protection (Amendment) Bill 2024 ("**Amendment Bill**") was passed by both chambers of the Malaysian Parliament. The Amendment Bill will be presented for Royal Assent and then gazetted. It will then come into force on an as yet unknown date to be gazetted by the Digital Minister.

The Amendment Bill aims to enhance PDP policies, particularly in terms of security and enforcement, to align Malaysia PDP laws more closely with international standards, and to address issues of personal data breaches and misuse in Malaysia.

The following paragraphs provide an overview of the PDPA, the amendments that will come into force, and the key subsidiary legislation, key principles, compliance and limitations.

#### a. Scope of Application

The PDPA is the primary law governing the processing of personal data, which is any information, data or chain of information that can be used to identify a living individual, in Malaysia. The PDPA applies to any person or organisation (referred to as a "data user" under the PDPA, which will be replaced by "data controller" when the Amendment Bill comes into force, to align with the more widely used terminology)[1] that processes, has control over, or authorises the processing of personal data in relation to commercial transactions in Malaysia, including foreign companies operating in Malaysia. Processing is broadly defined under the PDPA to cover a wide range of activities, including the collection, use, recording, storage, dissemination, rectification and/or erasure of personal data.

The Federal Government of Malaysia and State Governments are excluded from the application of the PDPA, as is any information processed for the purposes of a credit reporting business.[2]

#### b. General Principles

The PDPA sets out seven PDP principles that govern the processing of personal data by data controllers in Malaysia: consent, notice and choice, disclosure, security, retention, data integrity, and access. These principles aim to protect the privacy and personal information of individuals (**"data subjects"**) and ensure that they have control over how their personal data is used. Under the Amendment Bill, "data subjects" will now exclude deceased persons.

Under the PDPA, data controllers may not process the personal data of data subjects unless they have given their consent. However, there are certain exceptions data controllers may rely on to process personal data even without consent, such as when the processing is necessary for the performance of a contract to which the data subject is a party, to take steps at the request of the data subject with the intent to enter into a contract, to protect the "vital interests" of the data subject (where vital interest means matters relating to life, death or security of a data subject), or for the administration of justice. Consent is not defined under the PDPA, and the PDPA does not stipulate any requirements as to its form. but data controllers must be able to demonstrate that they obtained

1 For consistency, we will use "data controller" throughout this brochure.
2 Credit reporting businesses are, however, subject to similar laws under the Credit Reporting Agencies Act 2010.

consent and must allow data subjects to withdraw their consent. Therefore, consent may be orally given or implied so long as it is can be recorded. Nevertheless, it is often generally recommended that data controllers explicitly record consent received from data subjects in writing, e.g. through checkboxes or signatures. A data subject may withdraw his consent to the processing of his personal data by notice in writing.

The processing of sensitive personal data – that is, information concerning the physical or mental health or condition of the data subject, political opinions, religious or other beliefs of a similar nature, and starting with the Amendment Bill, biometric data – is subject to stricter safeguards under the PDPA. Processing of sensitive personal data requires explicit consent or must be necessary for employment, for the purposes of legal proceedings or legal advice, to protect the vital interests of the data subject or another person, or for medical purposes. The PDPA does not define what is meant by explicit consent, but it is generally understood that this means it can only be actively given and cannot be implied.

Companies must provide certain information to data subjects when collecting personal data. This includes a description of the data collected and the purpose(s) for which it is collected, the source of the personal data, the data subject's right to access and rectify their personal data, the class of third parties to whom their personal data may be disclosed, and a contact person to whom queries and complaints can be addressed. This information must be provided in both Bahasa Malaysia and English. Data controllers must also ensure that data subjects have the right to access their personal data and to correct their personal data if it is inaccurate, incomplete, misleading or not up to date.

The recent CTOS case,[3] which concerned inaccuracies in a plaintiff's credit rating and CTOS Data Systems Sdn Bhd's ("**CTOS**") failure to update her credit information despite being informed by the plaintiff that the data was inaccurate, highlights the importance of maintaining accurate data. The Malaysian High Court held that CTOS, which used personal data to establish credit ratings, had a duty of care to ensure that the information it provided about individuals was accurate and reliable. Although this case was decided under the Credit Reporting Agencies Act 2010 ("**CRA**") as it concerned a credit reporting agency, the PDPA contains similar provisions regarding data integrity and accuracy, and this ruling could potentially extend to personal data and data controllers. This means that organisations could potentially be exposed to negligence claims if they fail to maintain the accuracy and integrity of personal data, particularly in situations where the personal data is disclosed to third parties and influences third party decisions affecting the data subjects. To avoid the pitfalls of negligence, data controllers should implement rigorous data verification and updating protocols, prioritise responsiveness to feedback regarding the accuracy of the information they handle, and encourage the involvement of data subjects in maintaining the integrity of their own data.

There are currently no obligations for notification in the event of a breach, but data controllers may make voluntary notifications to the Personal Data Protection Commissioner (**"Commissioner"**). The Amendment Bill, on the other hand, makes the notification of personal data breaches to the Commissioner and to data subjects mandatory where a breach causes or is likely to cause significant harm. A personal data breach is defined as any breach, loss or misuse of personal data or unauthorised access to personal data. The amendments still do not specify a time limit within which the notification must be made.

The Amendment Bill also extends the obligations under the security principle to data processors. Data processors will now have the same direct obligations as data controllers to take practical steps to protect personal data and ensure its security. It is unclear to what extent, if any, this will relieve data users of their obligation to monitor their data processors. The amendments to the PDPA also introduce a new provision on data portability, giving data subjects the right to request the transfer of their personal data to another data controller, subject to technical feasibility and data format compatibility.

Finally, moving forward, organisations will also be required to appoint Data Protection Officers ("**DPO**"), who will have their own obligations to ensure the organisation's compliance with data protection law, as detailed in Part B.I.3.c below.

### c. Supporting regulations

The PDPA in Malaysia is supported by various subsidiary legislation and codes of practice. The subsidiary legislation sets out standards on security measures, data retention and data integrity, which apply to personal data that is processed electronically and non- electronically and are intended to be a "minimum requirement" for all data controllers. In addition, the subsidiary legislation defines the classes of data controllers required to register with the Personal Data Protection Commission under the PDPA are those in the communications

3 *Suriati v CTOS Data Systems Sdn Bhd* [2024] MLJU 437.

banking and financial, insurance, health, transport, education, direct selling, services, real estate, utilities, pawnbroking and money lending industries.

The General Code of Practice for the Protection of Personal Data (**"General CoP"**) issued by the Commissioner in support of the PDPA also came into force on 15 December 2022. The General CoP applies to categories of data controllers that are not currently subject to a specific code of practice under the PDPA.[4] The General CoP introduces more detailed legal requirements, including additional mandatory information for PDP notices, compliance with opt-out notices for direct marketing, the establishment of a personal data system and the development of a compliance framework. Given the potential criminal liability for non-compliance, companies subject to the General CoP should conduct a thorough internal review of their PDP policies and frameworks to ensure compliance with the new legal requirements.

### d. Compliance and enforcement

EU companies operating in Malaysia must comply with the PDPA to avoid penalties and to protect the personal data of individuals whose data they process. Directors and officers may also be held personally or jointly liable for offences committed by the company. Failure to comply with the principles of the PDPA can result in severe penalties, including fines, imprisonment, or both.

The Amendment Bill aims to demonstrate the country's commitment to stringent data protection enforcement by raising the maximum fine from MYR 300,000 to MYR 1 million and extending the maximum prison term from 2 to 3 years.

Enforcement of the PDPA is overseen by the Commissioner, who investigates complaints against non- compliant companies. Unlike the Companies Commission of Malaysia, the Commissioner does not have the power to impose fines, but may refer the matter to the Public Prosecutor. Any person aggrieved by the Commissioner's decision can appeal to the Appeal Tribunal. Despite being one of the first countries in Southeast Asia to have a data protection law, Malaysia's PDPA has several limitations.

### e. Limitations

Despite being one of the first countries in Southeast Asia to have a data protection law, Malaysia's PDPA has several limitations.

The PDPA has a limited scope and does not protect personal data beyond that processed for commercial transactions. The Federal Government is granted a blanket exemption and the PDPA does not apply to the State Governments either, which are likely to be the largest data processors in the country. In addition, as will be discussed in Part B.II the PDPA does not apply to data processed exclusively outside Malaysia, which is a notable gap given that major data breaches often involve transnational elements.

One of the biggest limitations of the PDPA has historically been the lack of enforcement, which was highlighted when a major telco data leak in 2017 compromised the personal information of 46 million mobile phone accounts. However, enforcement of data-related offences has been increasing, as illustrated by the recent high-profile cases involving Genting Malaysia Berhad and CTOS Data Systems Sdn Bhd.

## 2. The EU: the GDPR

The General Data Protection Regulation (**"GDPR"**), which was adopted by the European Parliament and the Council of the European Union on 14 April 2016 and became effective on 25 May 2018, is the main EU data protection regulation that gives individuals in the EU, and more broadly the European Economic Area ("**EEA**"), rights over how their personal data is processed, whether the processing takes place online or offline.

### a. General Principles

The GDPR protects personal data and outlines several requirements that businesses must follow in order to process data lawfully. Similar to the PDPA, "processing" is broadly defined to include, for example, collecting, recording, organising, storing, disclosing and deleting personal data. Data users are referred to as "data controllers" under the GDPR, and data processors – any third party that processes personal data on behalf of the data controller – are more widely regulated.

The GDPR involves minimising data collection and implementing security measures from the outset of processing to prevent data leaks and breaches at all stages of personal data processing. Data minimisation involves limiting the collection, use, and retention of personal data to what is necessary for a specific purpose. For instance, a data controller should collect only the personal data necessary to

4 There are six industry-specific codes of practice, covering the banking and financial sector, the utilities sector, the insurance and takaful industries, the communications sector, and private hospitals in the healthcare industry.

provide the specific service (e.g. name, phone number and address for on-site services, but not date of birth or nationality), rather than collecting a blanket list of personal data regardless of its necessity. Security measures include limiting the number of staff with access, encryption, pseudonymisation or anonymisation of data, etc.

The GDPR outlines six principles that summarise its requirements for personal data processing: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation and integrity, and confidentiality. Under the GDPR, personal data may only be processed if there is at least one legal basis for doing so, namely one of the following:

- the data subject has consented to the processing of their personal data for one or more specified 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 to comply with a legal obligation to which the controller is subject;
- processing is necessary 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 controller; or
- processing is necessary for the purposes of the legitimate interests pursued by the 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 the protection of personal data, in particular where the data subject is a child.

Many companies rely on obtaining users' consent to lawfully process personal data, which must meet the strict requirements of being freely given, specific, informed, and unambiguous as to the data subject's wishes. Data controllers must be able to demonstrate that they have obtained lawful consent, and must provide an easy way for data subjects to withdraw their consent. A data controller may not refuse service to users who refuse to consent to processing that is not strictly necessary for the use of the service.

The GDPR prohibits the processing of special categories of personal data, such as racial or ethnic origin, political opinions or genetic data, etc. (**"special data"**), as a default. However, if certain conditions are met, this data may be processed. Although the definition of special data is much broader, the conditions for processing are similar to the bases for processing sensitive personal data under the PDPA and include explicit consent of the data subject, processing for employment, social security, medical or legal purposes, and the protection of vital interests. Several additional exceptions also apply such as processing as part of a not-for-profit's body's legitimate activities.

Data subjects have several rights under the GDPR, including the right to access their personal data, rectify inaccurate information, erase personal data in certain situations, restrict processing, receive a portable copy of their data, object to processing, withdraw consent, and lodge a complaint with a data protection authority.

Companies must provide certain information to data subjects when collecting personal data. This includes the identity and contact details of the data controller, the purpose and legal basis for processing the data, information about any third parties who will receive the data, and how long the data will be stored. Data subjects also have the right to access personal data collected about them, to withdraw their consent to processing, and to request the erasure of their personal information. Controllers must also inform data subjects of the purposes for which their data is being processed, the categories of data being processed, who receives the data, how long the data will be stored and any automated decision- making processes used.

Under the GDPR, businesses are required to ensure the secure storage of personal data and protect it from data leaks or breaches. In the event of a data breach, companies must notify the relevant data protection authority within 72 hours, and if the breach is likely to result in a high risk to the rights and freedoms of natural persons, the individuals concerned must be notified as soon as possible

### b. Compliance and enforcement

Compliance with the GDPR is crucial to avoid potential sanctions and fines. Sanctions that can be imposed on organisations that breach its regulations include a written warning for first-time and non-intentional breaches, regular data protection audits, and fines. Fines can be up to EUR 20 million or up to 4% of the gross annual turnover of the previous financial year, whichever is higher, for some of the most severe infringements.

The GDPR is enforced by various data protection authorities in EU/EEA countries, which monitor the application of the GDPR and relevant national laws, provide advice on data protection issues, and handle complaints about breaches of the law.

## 3. Key differences between the PDPA and the GDPR

While both regulations aim to protect personal data, it is important to note that the GDPR is not restricted to personal data processed in the context of commercial transactions, is generally more detailed, and is considered to go further than the PDPA.

With the changes included in the Amendment Bill, such as the appointment of a DPO and the right to data portability, Malaysia appears to be taking steps towards the GDPR standard. Nevertheless, compliance with the GDPR does not necessarily mean compliance with the PDPA, as their provisions sometimes differ in material aspects. It is therefore important to be aware of these differences and ensure that your organisation complies with the relevant regulations to avoid legal issues.

Some examples of the differences between the two laws are outlined below.

### a. Basis for data processing

The default basis for data processing under the PDPA is the consent of the data subject. However, there are certain exceptions which allow data to be processed without consent, such as where the processing is necessary (i) for the purposes of a contract with the data subject, (ii) to take steps at the request of the data subject with a view to entering into a contract, (iii) to comply with a legal obligation to which the data controller is subject, other than an obligation imposed by a contract, (iv) to protect the vital interests of the data subject, (v) for the administration of justice, or (vi) for the exercise of functions conferred on any person by or under any law.

Under the GDPR, personal data can only be processed if there is at least one legal basis for doing so. Here, consent is merely one of several available bases, which are generally similar and include (i) necessity for the performance of a contract, (ii) compliance with a legal obligation, (iii) to protect the vital interests of the data subject or of another person, or (iv) the performance of a task carried out in the public interest or in the exercise of official authority. However, the GDPR also provides another basis for processing data that is not available under the PDPA: where processing is necessary for the purposes of the legitimate interests of the controller or a third party.

Legitimate interest can be defined as where the company's interest in processing the data is balanced against the individual's right to privacy. Under the GDPR, companies are required to conduct a legitimate interest assessment ("**LIA**") to determine whether their interest in processing the data outweighs the individual's right to privacy. The LIA should take into account factors such as the purpose of the processing, the nature of the data, the impact on the individual and any safeguards that can be put in place to protect the data. Companies should also provide individuals with information about their legitimate interests and their right to object to the processing of their data on legitimate interest grounds.

### b. Data portability

The GDPR explicitly grants individuals the right to request their personal data, which must be provided to them in a machine-readable format that can then be easily transferred to another data controller without compromising its usability or security. Data subjects can also request that the controller directly transmit this data to another controller.

The PDPA currently does not recognise data portability as a standalone right and only allows data subjects to request a copy of their personal data. The Amendment Bill, however, will give data subjects the right to request the transfer of their personal data to another data controller, subject to technical feasibility and data format compatibility (although there are currently no penalties for non-compliance).

Although this brings the PDPA closer to EU law, the Amendment Bill is much less detailed than the GDPR. For example, it does not impose any obligations as to the format in which data must be provided. In addition, the right of the data subject to receive their data themselves is covered separately from the right to have it transferred to another controller. For the former, the PDPA only says that the data must be "in an intelligible format", whereas the GDPR has the same requirements for providing copies of a data subject's data whether the data subject receives their personal data themselves or has it transferred directly to another controller.

### c. Data Protection Officers

Under the current version of the PDPA in force, DPOs are not mandatory in Malaysia. Instead, all companies must provide the details of a contact person who deals with queries and

complaints related to personal data. In addition, data controllers falling within certain categories (e.g. communications, banking and financial institutions, insurance, tourism, services, real estate, etc.) must register as data controllers with JPDP and appoint a "compliance person" who is identified as the person who will "oversee the application of the PDPA in the data controller's organisation".

However, the appointment of one or multiple DPOs will be mandatory once the Amendment Bill comes into force. The main task of the DPO will be to ensure that the organisation complies with data protection legislation. The Amendment Bill does not further define the duties of the DPO, nor does it prescribe any specific penalties for non-compliance.

The DPO is accountable to the controller or processor for compliance with the PDPA, but their appointment does not relieve the controller or processor of their duties and obligations under the law. It is so far unclear how far this accountability extends or whether it can be discharged.

Under the GDPR, organisations that process Special Data or monitor behaviour on a large scale must appoint a DPO to handle all GDPR activities and paperwork, monitor compliance, provide guidance, and communicate with authorities or data subjects as necessary. Even when not mandatory, the appointment of a DPO is recommended as best practice to ensure compliance with the GDPR.

Organisations outside the EU that are subject to the GDPR must also generally also appoint an EU-based representative to fulfil their GDPR obligations. Failure to do so may result in fines, and intentional or negligent breaches may constitute aggravating factors. However, entities carrying out occasional processing that does not involve special categories of data or processing of personal data relating to criminal convictions and offences may be exempt from appointing an EU representative. Non-EU public authorities and bodies are also exempt.

As with data portability, the PDPA is much less precise than the GDPR. It merely instructs companies to designate a DPO without offering the level of details found in the GDPR regarding the actual implementation, e.g. the DPO's tasks, the qualifications necessary for their appointment, the management of the relationship between the DPO and the controller / processor, the DPO's obligations concerning confidentiality, secrecy, and independence, etc.

As no geographical requirements currently exist for DPOs, multinational groups may consider a group-wide DPO that fits into the existing corporate structure of the entire group, centralising policies and information. However, any DPO appointed must be sufficiently qualified, knowledgeable and empowered to carry out their duties as DPO. In particular, the DPO will need to be aware of country-specific requirements and keep up to date with the PDP laws of all jurisdictions they cover. They must also be able to respond quickly to requests from different countries and time zones, as some response deadlines may be short (e.g. 14 days under the PDPA). In addition, a group-wide position will almost always result in cross-border data transfers, for which the necessary documentation should be in place (as detailed in Part B.II below).

The DPO does not need to be an employee of the organisation and their responsibilities may be outsourced to local firms with the relevant expertise.

Even when not legally mandated, a local DPO (or other personal data protection position) can help European companies navigate the complexities of the GDPR and the PDPA, ensure that their data protection practices comply with the law, help companies protect their customers' personal data, and avoid legal and reputational risks.

### d. Extra-territorial application

The PDPA does not apply to personal data processed outside Malaysia, unless the data is intended to be further processed in Malaysia, nor does it apply to a data controller 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.

On the other hand, although adopted in the EU, the GDPR affects organisations worldwide. The protections of the GDPR apply to any individual physically located in the EU or the EEA, regardless of nationality, citizenship status or whether their data is processed online or offline. The GDPR must also be complied with by all businesses established in the EU/ EEA, regardless of whether the data processing takes place inside or outside this region.

Furthermore, businesses that are not established in the EU/ EEA may still fall within the legal scope of the GDPR if they offer goods or services that are available to individuals in the EU/EEA, monitor the behaviour of individuals in this region, or use data processors based in the EU. This means that businesses located anywhere in the world may potentially be required to comply with the GDPR. Therefore, Malaysian businesses that provide goods or services to, or monitor the behaviour of, EU residents will need to comply with the GDPR.

This may affect corporate groups with operations in both Malaysia and the EU, either internally or directly depending on the structure of their operations, as well as Malaysian companies that directly engage in activities such as tracking EU citizens' data online (e.g., by tracking website visitors) or catering to customers in the EU (which may include, for example, creating advertisements in EU languages, particularly those not spoken outside of the EU, quoting prices in EU currencies, advertising their services as being provided in the EU, etc. In general, one indicator alone will not be sufficient and several should be present).

However, it is still uncertain to what extent the EU or its Member States will be able to enforce the GDPR against organisations that do not have a presence in the EU.

## II. Cross-border data transfers

Cross-border data transfers between Malaysia and the EU are subject to different rules depending on the direction of the transfer. When personal data is transferred from Malaysia to the EU, the transfer is subject to the PDPA, while transfers from the EU to Malaysia are subject to the GDPR.

### 1. Transfers from Malaysia to the EU

Currently, the PDPA prohibits the transfer of personal data from Malaysia to any other country, except to a country specified by the Minister and published in an official gazette ("**white-list**"). No countries have been officially designated since the creation of the white-list.

Notwithstanding this general prohibition on the transfer of personal data out of the country, the PDPA provides for a number of exceptions, such as where the consent of the data subject has been obtained for such transfer and where the transfer is necessary for the performance of a contract between the parties. If there is any doubt as to whether the data transfer exceptions apply, the prudent approach is to obtain the data subject's consent to such transfer outside Malaysia. In relation to outsourcing, a data controller is not permitted to transfer data to third parties unless the data subject's consent has been obtained. In addition, for all transfers to third parties, the data controller must 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 complies with those measures.

Following the Amendment Bill, the white-list system will be abolished and personal data may be transferred from Malaysia to any country with "substantially similar laws" or "ensuring an equivalent level of protection" – although it is not clear what the criteria will be for laws to be considered similar or ensuring equivalent protection nor whether this will be up to companies to assess or whether there will be controls. The rest of the provisions on transfers remain in force, including the ability to use the exceptions as a basis for transfer outside of Malaysia.

In relation to transfers to the EU, the GDPR is likely to be regarded as substantially similar and ensuring equivalent levels of protection, but it remains to be determined how this will be assessed and by whom, and how organisations will be expected to demonstrate this.

Although not envisaged in Malaysian law, the Association of Southeast Asian Nations ("**ASEAN**") had developed a set of Model Contractual Clauses for Cross-Border Data Flows ("**MCCs**") that can be included in the contracts of parties transferring personal data across borders. The MCCs set out the responsibilities of the parties and require PDP measures, covering different transfer scenarios. These clauses are intended to help the parties ensure that the transfer of personal data is done in a manner that complies with the legal and regulatory requirements of ASEAN member states, protects the data of data subjects, and promotes citizen confidence in the ASEAN digital ecosystem.

### 2. Transfers from the EU to Malaysia

Under the GDPR, the transfer of personal data of EU data subjects to countries outside the EU/EEA, known as "third countries", is prohibited unless (i.) the third country's data protection regime is formally assessed by the European Commission as adequate and an adequacy decision is issued or (ii.) adequate safeguards are in place.

The GDPR sets out non-exhaustive criteria for the Commission to consider when making an adequacy decision on the level of data protection in a third country or international organisation. In particular, the third country must ensure an effective data protection system and the existence of effective data protection supervision, as well as the existence of international commitments in relation to the protection of personal data.

Examples of appropriate safeguards in the absence of an adequacy decision include binding corporate rules for intra-group transfers, standard contractual clauses ("**SCCs**") on data protection (either as a standalone contract or as part of a data processing agreement ("**DPA**") or wider contract), or a scheme of binding and enforceable commitments by the controller or processor located in a third country.

Since the Court of Justice of the European Union's Schrems II decision in 2020,[5] which invalidated the legal framework regulating and ensuring an adequate level of protection for the exchange of personal data for commercial purposes between the EU and the United States (known as the "EU-US Privacy Shield"), the use of SCCs requires more forethought. While SCCs remain valid in principle as a transfer mechanism, and new SCCs were adopted by the EU on 4 June 2021, they cannot be used without additional investigation.

Companies considering cross-border data transfers must ensure that the recipient countries provide data protection equivalent to that in the EU by carrying out Transfer Impact Assessments ("**TIAs**"). Organisations relying on SCCs must assess, on a case-by-case basis and, where appropriate, in cooperation with the recipient of the data, whether the law of the third country of destination ensures an adequate level of protection for personal data transferred under the standard data protection clauses. If not, additional safeguards must be added to the SCCs and if no safeguards can be achieved, the data should not be transferred at all. If the existence security and surveillance laws would prevent compliance with the GDPR, then the exporter must stop the transfer and terminate the contract. If the data exporter fails to comply with its obligations, the Lead Supervisory Authority, the GDPR's main regulatory body, may intervene and/or prohibit the transfer.

As Malaysia is currently a third country without an adequacy decision, the transfer of personal data from EU/EEA countries to Malaysia, including between group companies, is limited to situations where adequate safeguards are in place, meaning that SCCs and TIAs are required.

The European Commission recommends using the EU template SCCs as provided to ensure compliance with the GDPR, with the only adaptations to be made being those already envisioned in the templates depending on the nature of the transfer (e.g. controller-to-controller, controller-to-processor, etc.).

Although there are some common bases for transfers and data processing agreements, legal and regulatory frameworks differ from region to region and require different safeguards and contractual provisions to ensure compliance.

# C. Use and Regulation of Data

While personal data is the most regulated form of data due to its sensitivity and potential impact on individuals, other uses of data have also become more regulated. It is important for companies to consider what happens to the data they collect in general, as its use and protection is more and more regulated. In the European Union, various laws have been implemented to regulate the use of data and protect the privacy of individuals. This means that data in general is now more heavily regulated, and it is important to be aware of how these regulations may apply to you or your group companies, which may require you to comply with certain data protection measures. This section will explore the regulations that apply to data other than personal data and what they mean for your business.

A broader issue surrounding the use and regulation of data is also how it is stored and protected. As a result, cybersecurity laws are becoming increasingly common, requiring organisations to implement security controls to protect against cyber threats and data breaches.

## I. Data Act

The European Union has recently taken an important step towards a data-driven future with the introduction of the Data Act. This regulation aims to modernise and standardise data governance across the EU, playing a pivotal role in shaping the digital economy and society over the next decade. The following paragraphs cover some of the key highlights and objectives of the Act that businesses need to be aware of.

### 1. Background

The Data Act was adopted on 27 November 2023, came into force on 11 January 2024 and will become applicable on 12 September 2025. The Act applies to manufacturers of connected devices (such as IoT and medical devices, but also connected vehicles), data processing services such as cloud service providers and their users, public sector bodies and others.

### 2. Key provisions

The Data Act aims to complement the GDPR and clarify who owns the data generated by internet-connected devices, such as cars, appliances, and industrial machinery. It gives users of connected devices, ranging from smart household appliances

5 Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*, ECLI:EU:C:2020:559 (July 16, 2020).

to intelligent industrial machines, the right to gain access to data generated by their use and to share it with other service providers, with the aim of boosting competition, unlocking the potential of non-personal data, and keeping pace with the United States in the battle for AI-driven productivity gains.

The Data Act requires product and related service data to be made available to users in a secure, structured, commonly used and machine-readable format, free of charge, of the same quality as that available to the data holder and where technically feasible directly, continuously and in real time. It also gives individuals and businesses a strengthened portability right to copy and transfer data across different services and providers of data processing service. Certain sectors, e.g. smart cars, will have sector-specific rules.

Access, use or further transfer of data may be contractually restricted or prohibited if it could undermine security requirements, resulting in a serious adverse effect on the health, safety or security of natural persons. The data holder may also refuse a request for access to data if it holds trade secrets and can demonstrate that, despite the measures taken by the user, disclosure of its trade secrets is likely to cause serious economic harm. The data holder must notify the user and the competent authority in writing if data sharing is refused, and the user may challenge the decision by lodging a complaint with the competent authority or by agreeing with the data holder to refer the matter to a dispute resolution body.

In addition, the new law contains measures to prevent the abuse of contractual imbalances in data sharing contracts due to unfair terms imposed by a party with a significantly stronger bargaining position by requiring manufacturers and service providers to provide information about the data related to the purchase or service before a contract is concluded. The Act also includes provisions for certain EU and national public bodies to request data during emergencies, addresses the cloud market and switching between cloud providers, and includes a chapter on automated “smart contracts”.

The Data Act covers both personal and non-personal data, but compliance with the GDPR is still required for the processing of personal data, as the Data Act does not provide a legal basis for the collection or generation of personal data, nor does it give data holders new rights to use personal data. Data holders can comply with requests for access to personal data by anonymising it, or by transmitting only data relating to the user. Technical measures to comply with data protection principles may include pseudonymisation, encryption and the use of technology to process necessary data.

## 3. Key objectives

The Data Act has a number of objectives:

- Complementing the Data Governance Regulation: While the Data Governance Regulation focuses on processes and structures to facilitate data, the Data Act clarifies who can create value from data and under what conditions.
- Empowering data generation: The Data Act aims to provide legal certainty for businesses and consumers on the use of data. It encourages producers to invest in high-quality data generation, promotes a fair distribution of data capacity and encourages digitisation.
- Preventing abuse and ensuring fairness: The Data Act tackles contractual imbalances that prevent fair data sharing. Small and medium-sized enterprises (**“SMEs”**) will be protected from unfair contractual terms imposed by stronger market players. In addition, the Commission will develop model contract clauses to facilitate fair data sharing agreements.
- Public sector access: The law allows public sector bodies to access and use data held by the private sector for specific public interest purposes. This access could help develop insights to respond quickly and securely to public emergencies, while minimising the burden on businesses.
- Unlocking the EU cloud market: New rules will set the framework for customers to effectively switch between different providers of data processing services, contributing to an efficient EU cloud market and overall data interoperability.
- Clarifying the Database Directive: The Data Act clarifies that the *sui generis* database rights (the right to protect the content of certain copyrighted and non-copyright eligible databases) harmonised under the Database Directive does not apply to databases created from data generated or obtained by IoT devices.

The Act also establishes a Data Access and Portability Authority to monitor compliance and enforce penalties for non-compliance.

## 4. Impact on businesses

The Data Act is expected to have a significant impact on businesses operating in the EU. It could create new opportunities for data-driven innovation, but it also imposes new obligations and requirements on many industries. The law requires companies to provide individuals with access to their data in a clear and easily accessible manner, and to give individuals the right to transfer their data to other service providers.

The law targets virtually every sector in Europe, including vehicles, windmills, industrial robots, connected devices, smart speakers or watches. The law aims to mandate data sharing, which could give some, such as transport operators, access to data that was previously difficult to obtain. However, many industry heavyweights expressed concern that mandating data sharing could expose commercially sensitive data and lead to copycat technologies competing with European companies' innovations. Final negotiations on the bill focused on the protection of trade secrets, with EU countries seeking an exemption from data sharing if disclosure of those secrets would cause "serious harm", while lawmakers feared this could create a loophole.

Overall, the EU Data Act represents a significant opportunity for the EU to establish itself as a global leader in data governance and may inspire similar legislation across jurisdictions. However, careful planning and implementation will be required to realise its full potential. Given the transition period of less than two years, organisations should start preparing now for its implementation and ensure compliance with the new rules.

### 5. Impact in Malaysia

Although the Data Act is specifically designed for EU Member States, it also has implications for non-EU jurisdictions, including Malaysia. The Data Act, similar to the GDPR, applies to manufacturers of connected products and providers of data processing services offered in the EU market, regardless of where they are based. Therefore, non-EU companies that intend to sell connected products or provide data processing services to individuals in the EU should be aware of the new regulation and consult with legal experts to ensure that the company is compliant with all relevant legislation.

One of the main implications of the Data Act for non-EU countries relates to the export of data. If data is to be stored or processed outside the EU, the restrictions on exporting data to non-EU countries must be taken into account. In particular, providers of data processing services must take appropriate technical, organisational, and legal measures, including contractual clauses, to prevent foreign and governmental access to and transfer of non-personal data held in the EU where such transfer or access would be contrary to either EU law or the national law of the Member State concerned.

## II. Data Governance Act

The Data Governance Act (**"DGA"**) is an EU regulation that aims to create a framework to facilitate data sharing, increase trust in data sharing, strengthen mechanisms to increase data availability and overcome technical barriers to re-using data.

### 1. Background

The DGA was adopted on 30 May 2022 and has been in force since 24 September 2023. It was introduced with the aim of creating a framework to increase trust in voluntary data sharing for the benefit of businesses and citizens in the EU. The EU considers that the economic and societal potential of data is enormous, but that barriers such as low trust in data sharing, issues related to the re-use of public sector data and data collection for the public good, as well as technical barriers, prevent its full potential from being realised.

The DGA is meant to address these barriers by providing rules and safeguards that make it easier to share data in a trusted and secure way.

### 2. Key Provisions

The DGA has three main components:

- Re-use of certain categories of data held by public sector bodies: The DGA provides rules and safeguards to facilitate the re-use of protected data (e.g. personal data and commercially confidential data) held by public sector bodies that cannot be re-used as open data, but could be re-used under specific EU or national legislation. Technical requirements and assistance will also be provided by the public sector body to ensure that the privacy and confidentiality of the data are fully respected in re-use situations. Reasonable fees may be charged, but public sector bodies should encourage re-use for scientific research and other non-commercial purposes, as well as by SMEs and start-ups.
- Data intermediation services: In order to ensure that data intermediaries act as trusted organisers of data sharing or pooling within the common European data spaces, the DGA defines a set of rules for data intermediary service providers (such as data marketplaces). Data intermediaries must comply with strict requirements to ensure neutrality and avoid conflicts of interest. Data intermediaries may charge for facilitating the exchange of data between parties, but they may not directly use the data they broker for financial gain.
- Data altruism: Data altruism involves individuals and companies giving their consent or permission to make data they generate voluntarily and without payment available for use in the public interest. The DGA provides trusted tools that make it easy to share data for the benefit of society.

Organisations that make relevant data available on the basis of data altruism can register as "Data Altruism Organisations Recognised in the Union". They must be non- profit making and comply with a set of rules developed by the Commission.

### 3. Data Exchanges

The DGA provides for the establishment of the European Data Innovation Board (**"EDIB"**) to facilitate the exchange of best practices, in particular on data brokerage, data altruism and the use of public data that cannot be made available as open data, as well as the prioritisation of cross-sector interoperability standards. The EDIB includes representatives from the competent authorities of the EU Member States, the European Data Protection Board, the European Data Protection Supervisor, the EU Agency for Cybersecurity, the European Commission, the EU SME Envoy and other relevant bodies.

The DGA provides safeguards for access requests from third countries in the context of non-personal data and allows the Commission to make available model contractual clauses for public sector bodies and re-users for scenarios where public sector data is involved in data transfers with third countries. The DGA also provides a framework to increase trust and confidence in voluntary data sharing for the benefit of businesses and citizens by addressing barriers that limit data sharing in the EU, and its components provide rules and safeguards to facilitate data sharing in a trusted and secure way.

The DGA applies to both personal and non-personal data, and where personal data is involved, the GDPR applies concurrently.

## III. Cybersecurity Legislation

Data protection and cybersecurity laws both aim to protect sensitive information from unauthorised access, use or disclosure. While data protection laws establish rules for the collection, processing and storage of personal data and often require the implementation of certain security measures to protect personal data, cybersecurity laws create frameworks and oversight bodies for the implementation of security controls and the prevention of cyber threats and data breaches in general. Organisations can maximise the protection of their data and information systems by complying with both sets of legislation.

Since 2019, the EU has had cybersecurity legislation in the form of the Cybersecurity Act, which aims to strengthen the EU's cybersecurity posture and protect the digital single market. It establishes a framework for EU-wide cybersecurity certification, and gives the European Union Agency for Cybersecurity a mandate to support member states in their cybersecurity efforts. The Act also creates a European Cybersecurity Certification Framework: a set of rules, technical requirements, standards, and evaluation procedures that apply to the certification of specific ICT products, services, or processes and attest that the product, service, or process has been certified in accordance with the requirements and rules of the scheme. In addition, the Cybersecurity Act introduces a voluntary EU-wide cybersecurity information sharing mechanism, which will allow Member States and the private sector to share information on cybersecurity threats and incidents.

The Malaysian Parliament, on the other hand, passed a new Cybersecurity Bill on 3 April 2024, which proposes to establish a comprehensive legislative framework to combat cybercrime. The Bill is intended to serve as an overarching cybersecurity law with extraterritorial application, which applies irrespective of nationality or citizenship and outside Malaysia, where an offence under the Act is committed in relation to a National Critical Information Infrastructure ("**NCII**") located wholly or partly in Malaysia. The Bill defines NCII as a computer or computer system, the disruption or destruction of which would have a detrimental effect on the provision of services essential to the security, defence, foreign relations, economy, public health, public safety or public order of Malaysia and already identifies certain specific sectors as NCIIs, such as banking, finance, transport, information, digital, communications, trade, industry, commerce, science, technology, innovation, etc. NCII entities are expected to implement measures, standards and processes to ensure the cybersecurity of their NCII. Alternative measures may be implemented if the entity can demonstrate to the Chief Executive of the National Cyber Security Agency that they provide an equivalent or higher level of protection. Entities will also be required to provide information about their NCII, conduct cybersecurity risk assessments, carry out cybersecurity exercises, and notify the Chief Executive and the NCII Sector Lead of any cybersecurity incidents.

The Bill also proposes to establish a licensing regime for cybersecurity service providers, although what constitutes a cybersecurity service or what the licence application would look like has not yet been defined. The Bill would also establish the National Cyber Security Committee, comprising various ministerial stakeholders, and strengthen the National Cyber Security Agency as the lead cybersecurity agency in Malaysia

# D. Artificial Intelligence

Artificial intelligence ("**AI**") has transformed industries and societies worldwide, and Malaysia is no exception. Malaysia is poised to generate as much as USD 113.4 billion in productive capacity – a quarter of the country's 2023 gross domestic product – through the adoption of generative AI. However, as the use of AI grows, so too do concerns about the protection of personal data.

Data is a fundamental element in the development and implementation of AI. AI systems rely on large amounts of data to learn and improve their performance. This data can come from a variety of sources, including personal information about individuals, such as their name, address, phone number, and other sensitive data. The use of personal data in AI raises concerns about privacy, security and the potential misuse of such data.

And so, as AI continues to permeate different sectors and domains, it has become increasingly important to regulate its use to ensure that it is safe, ethical, and transparent. In recognition of this need, the EU introduced the Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence or "**AI Act**" in April 2021, which aims to provide a harmonised regulatory framework for AI across the EU and beyond. The EU AI Act is a landmark legislation that sets out a "risk-based" approach to regulating AI and defines several categories of AI systems with varying levels of risk and scrutiny.

While the EU AI Act is primarily aimed at the EU, it may have implications for companies doing business in or with countries, such as Malaysia, that have business links with the EU and share similar concerns about the regulation of AI.

## I. EU Artificial Intelligence Act

The EU AI Act is a new and comprehensive regulation that aims to create a legal framework for the development and use of AI in the European Union. The EU Commission proposed the Act in April 2021, and it was adopted by the European Parliament on 13 March 2024 and subsequently approved by the Council of the EU on 21 May 2024. It came into force on 1 August 2024.

Its provisions will become applicable in stages, with delays varying depending on the type of application: 6 months for bans on "unacceptable risk" AI systems, 9 months for codes of practice, 12 months for general purpose AI systems, 24 months for everything else, and 36 months for some obligations related to "high risk" AI systems. To bridge the transition period before full implementation, the Commission has launched the AI Pact, an initiative inviting AI developers to voluntarily adopt key obligations of the AI Act ahead of the legal deadlines.

The AI Act is a historic move towards regulating the development and use of AI. It covers a wide range of applications of AI, including machine learning, natural language processing, and robotics. The Act follows OECD criteria to distinguish AI from simpler software systems. It does not apply to areas outside EU law, to AI used exclusively for military or defence purposes, to non-professional use of AI, or to research and innovation. It also makes clear that it is not intended to interfere with the competences of Member States in the area of national security, or with bodies entrusted with tasks in this area.

The Act establishes a protective framework for AI that includes a tiered approach to address different levels of risk. AI systems will be categorised according to their level of risk. Low-risk AI systems are subject to minimal transparency requirements, only disclosing AI-generated content for user awareness. High-risk AI systems will be able to enter the EU market, but will have to comply with clarified and technically feasible requirements, which will reduce the compliance burden.

The AI Act's key provisions include:

- Risk-based approach: The AI Act adopts a risk-based approach to regulating AI, meaning that AI systems that pose a high risk to people or society are subject to stricter requirements and more rigorous testing.
- Prohibition of certain AI practices: The AI Act prohibits certain AI practices that are deemed unacceptable, such as AI systems that manipulate human behaviour or use subliminal techniques to exploit vulnerabilities in human decision-making.
- Obligations for high-risk AI systems: The AI Act sets out a number of obligations for high-risk AI systems that pose a risk to people's health, safety, or fundamental rights, including requirements for transparency, documentation and human oversight.
- Conformity assessment: Companies that develop or market AI systems that pose a high risk must undergo a conformity assessment process to ensure that their systems comply with the requirements set out in the AI Act.
- Enforcement and penalties: The AI Act provides for enforcement measures and penalties for non-compliance, including fines of up to 6% of a company's annual global turnover.

## II. Impact in Malaysia

Currently, there are no specific laws in Malaysia that deal with AI. The Minister of Science, Technology and Innovation has indicated plans to consult with experts and stakeholders in the field and to draft a comprehensive AI Bill to address aspects such as privacy, transparency, accountability and cybersecurity risks.

### 1. Impact on the legal landscape

The EU AI Act may influence Malaysia's approach to regulating AI when developing its proposed AI bill. Malaysia has already developed a Malaysia Artificial Intelligence Roadmap 2021-2025, which provides a framework for the adoption of AI across many sectors of the economy, and is considering AI- related legislation. The AI Act provides concrete legislation and sets a higher standard for the development and use of AI systems, which may encourage Malaysia to adopt concrete and robust AI regulations more quickly.

Furthermore, the AI Act also provides an opportunity for Malaysia to align its AI regulations with those of the EU, which could facilitate trade and cooperation between the two regions.

Until any such AI-specific regulation is implemented, the laws which regulate the use of data, which is both a crucial component of AI and a potential vulnerability, may apply to companies processing data through AI, as AI tools can be susceptible to data breaches.

The PDPA requires organisations to obtain consent from individuals before collecting their personal data and to ensure that the data is used and disclosed only for the purposes for which it was collected. This could mean that, if personal data will be processed through AI or used to train AI systems, data controllers should inform data subjects of this use when collecting consent and ensure that the AI does not process personal data beyond the scope of the data subject's consent. The PDPA principles relating to the security and integrity of personal data will also be directly relevant when AI is used to process personal data.

### 2. Impact on Malaysian businesses

The EU AI Act could have a significant impact on Malaysian companies and other companies operating in Malaysia, regardless of Malaysian law. The AI Act sets out strict rules for the development, deployment and use of AI in the EU, so Malaysian companies which develop or market AI systems that are sold or used in the EU will need to comply with the requirements set out in the AI Act. This means that they will need to ensure that their AI systems are transparent, accountable, and unbiased. They will also need to carry out risk assessments and obtain appropriate authorisations before deploying AI systems in the EU. Companies serving both EU and non-EU markets may also want to consider whether to have only EU-compliant AI systems or several systems for different markets.

On the other hand, companies that comply with the AI Act's requirements may be able to use this to demonstrate to their customers and stakeholders that they take their responsibilities seriously and are committed to ethical and responsible AI practices. Demonstrating that their AI systems meet the standards required by the EU may also help Malaysian companies expand their business and reach new markets in the EU.

# E. Your contact persons

If you have any questions or require assistance with data protection matters, do not hesitate to contact us:

**Pascal Brinkmann, LL.M. (Stellenbosch)**
Partner
pascal.brinkmann@luther-services.com

**Lukas Kirchhof, LL.M. (Chinese University of Hong Kong)**
Senior Legal Counsel
lukas.kirchhof@luther-services.com

**Shi Yin Khoo, MA (Cantab)**
Senior Legal Counsel
shiyin.khoo@luther-services.com

**Julie Schwarz, LL.M. (Georgetown)**
Legal Counsel
julie.schwarz@luther-services.com

# Hits the mark. Luther.

Luther Rechtsanwaltsgesellschaft mbH is one of the leading corporate law firms in Germany. With some 420 lawyers and tax advisors, we can advise you in all fields of German and international corporate law. In addition to having offices in every economic centre throughout Germany, we are also present in 11 locations abroad: in Brussels, London and Luxembourg in Europe, and in Bangkok, Delhi-Gurugram, Ho Chi Minh City, Jakarta, Kuala Lumpur, Shanghai, Singapore and Yangon in Asia.

Our advisory services are tailored to our clients' corporate goals. We take a creative, dedicated approach to achieving the best possible economic outcome for each of our clients. The name "Luther" stands for expertise and commitment. With a passion for our profession, we dedicate all our efforts to solving your issues, always providing the best possible solution for our clients. Not too much and not too little – we always hit the mark.

We know how crucial it is to use resources efficiently and to plan ahead. We always have an eye on the economic impact of our advice. This is true in the case of strategic consulting as well as in legal disputes. We have complex projects on our agenda every day. At Luther, experienced and highly specialised advisors cooperate closely in order to offer our clients the best possible service. Thanks to our fast and efficient communication, permanent availability and flexibility, we are there for you whenever you need us.

**Lawyers and tax advisors**

**420**

**Locations**

**21**

**Long-standing connections to commercial law firms worldwide**

**Offices in international financial centres and investment locations**

# About unyer

unyer is a global organisation of leading international professional services firms. Besides law firms, unyer is also open to other related professional services, especially from the legal tech sector. unyer is based in Zurich as a Swiss Verein. unyer is globally connected but has strong local roots in their respective markets.

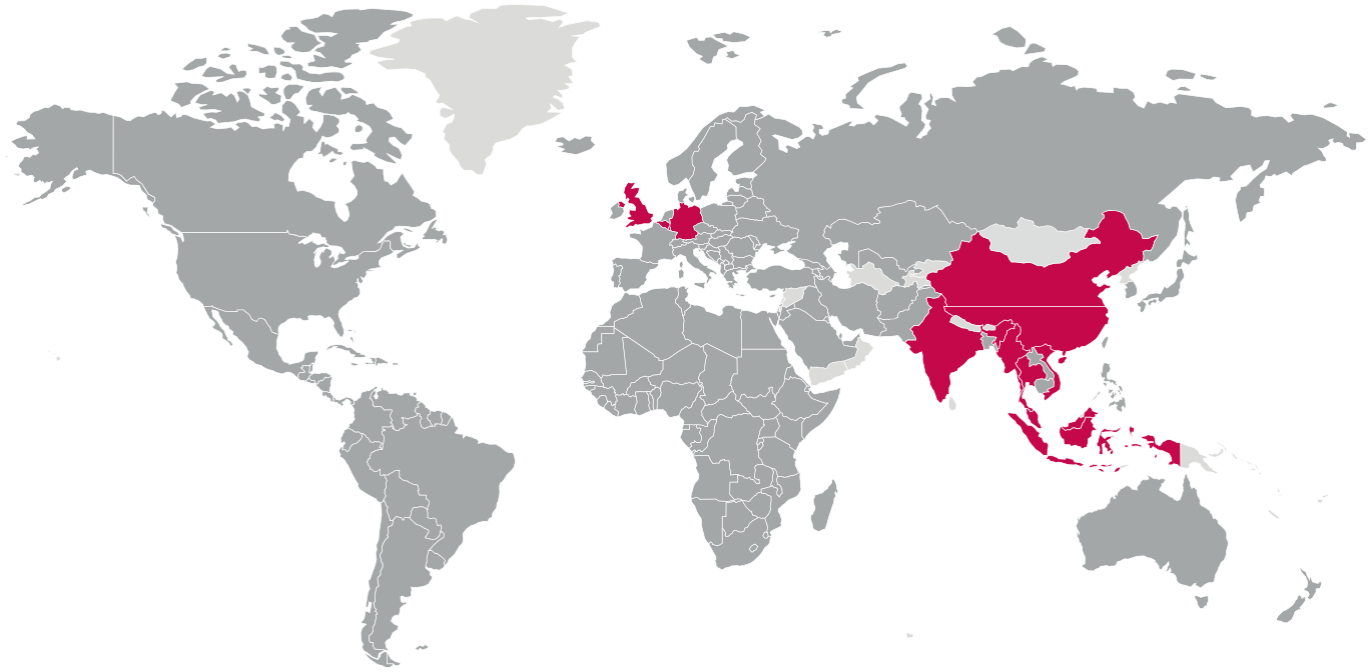
unyer has an exclusive approach and only accepts one member firm from each market. unyer members offer its clients full services across all jurisdictions with a compelling industry focus. The organisation has an annual turnover of more than EUR 650 million and includes over 2,550 lawyers and advisors in more than 14 countries in Europe and Asia. In September 2021, Pirola Pennuto Zei & Associati joined the international organisation. In the spring of 2023, the Austrian law firm KWR joined the group. www.unyer.com

MEMBER OF unyer

# Our locations

We have a global outlook, with international offices in 11 key economic and financial centres in Europe and Asia. We also maintain close relationships with other commercial law firms in all relevant jurisdictions. Luther is a founding member of unyer (www.unyer.com), a global organisation of leading professional services firms that cooperate exclusively with each other. This way, we ensure a seamless service for our clients throughout their demanding international projects.

Our partner firms are based in Africa, Australia and New Zealand, Europe, Israel, Japan and Korea, the Middle East, Russia and the CIS, South and Central America, the US and Canada.



Luther locations
Best friends

## Our locations

**Bangkok**
**Berlin**
**Brussels**
**Cologne**
**Delhi-Gurugram**
**Dusseldorf**
**Essen**
**Frankfurt a.M.**
**Hamburg**
**Hanover**
**Ho Chi Minh City**
**Jakarta**
**Kuala Lumpur**
**Leipzig**
**London**
**Luxembourg**
**Munich**
**Shanghai**
**Singapore**
**Stuttgart**
**Yangon**

# Our awards

### JUVE

In the JUVE Handbook of Commercial Law Firms 2023/2024, 53 lawyers were recommended by Luther, nine of whom were recognised as “Leading Advisors” and two as “Rising Star”. In total, Luther was ranked in 31 practice areas. In 2023, Luther was named “Law Firm of the Year for Procurement Law” and “Law Firm of the Year for Distribution, Trade and Logistics” by JUVE-Verlag. In addition, Luther was nominated as “Law Firm of the Year for Technology and Media”. In 2019, Luther received the highest award as “Law Firm of the Year 2019” from JUVE-Verlag.

### Chambers

In 2024, Luther was recognised by Chambers Europe for 14 practice areas in Germany as well as in two practice areas in Luxembourg. In addition, 20 partners were included in the Individual Ranking. Moreover, in 2024, Luther was recognised by Chambers Global in two practice areas in Germany and in one each in Luxembourg and Myanmar, while seven partners were also included in the Individual Ranking.

### The Legal 500

The Legal 500 Germany 2024 recommends Luther in 37 areas of law, with “Top Tier” rankings in two of these areas. 73 lawyers are being recommended, 16 of whom have been specially recognised as “Leading Individual” or “Next Generation Partner”. “The Legal 500 EMEA 2024” recommends Luther for seven areas of law in Luxembourg, and nine lawyers are also recommended, two of whom have been specially recognised as “Leading Individual”. “The Legal 500 Asia Pacific 2024” recommends Luther and two of its lawyers for one area of law in Myanmar.

### The Legal 500 Green Guide EMEA 2024

Luther has been included in the Legal 500 Green Guide EMEA 2024 for Germany, with three lawyers being recommended. The guide provides an overview of the law firms’ engagement with sustainability and covers both corresponding activities for clients and their own best practices and initiatives.

### Kanzleimonitor

Kanzleimonitor 2023/2024 recommends Luther in 20 areas of law and has also included four Luther lawyers among the recommended lawyers mentioned by name.

### „Best Lawyers in Germany 2024“

For the year 2024, 99 lawyers have been recommended by Luther as “Best Lawyers in Germany 2024”, an award presented by the US publisher “Best Lawyers” in cooperation with the German Handelsblatt, including one partner as “Lawyer of the Year” for his area of law, and 19 colleagues who have received the recommendation “Best Lawyers - Ones to Watch”.

### WHO’S WHO LEGAL

WHO’S WHO LEGAL lists a total of 23 lawyers in December 2023, six of whom received the highest award Thought Leader and three of whom were recognised as Future Leaders.

## Imprint

Luther Rechtsanwaltsgesellschaft mbH, Anna-Schneider-Steig 22, 50678 Cologne, Germany, Phone +49 221 9937 0, Fax +49 221 9937 110, contact@luther-lawfirm.com

Luther Corporate Services Sdn. Bhd. (200901028935 (872040-W)), Unit No. L25-1, Level 25, TSLAW Tower, No. 39, Jalan Kamuning, 50450 Kuala Lumpur, Tel +60 3 2166 0085, Fax +60 3 2166 0087, malaysia@luther- services.com



## Disclaimer

Luther.

**Bangkok, Berlin, Brussels, Cologne, Delhi-Gurugram, Dusseldorf, Essen, Frankfurt a.M., Hamburg, Hanover, Ho Chi Minh City, Jakarta, Kuala Lumpur, Leipzig, London, Luxembourg, Munich, Shanghai, Singapore, Stuttgart, Yangon**

You can find further information at:
www.luther-lawfirm.com
www.luther-services.com

unyer GLOBAL ADVISORS