

# DATA PROTECTION NOTICE

## EUROPEAN UNION AND UNITED KINGDOM

EFFECTIVE JANUARY 2025 (AS AMENDED)

### 1. INTRODUCTION

The purpose of this Data Protection Notice (this "**Notice**") is to inform the clients of:

- Morgan, Lewis & Bockius LLP, with branch offices at
  - 7 Rue Guimardstraat, B-1040 Brussels and enterprise number 0538 386 919, and
  - OpernTurm, Bockenheimer Landstrasse 4, 60306 Frankfurt am Main, Germany,
  - Königinstraße 9, 80539 Munich, Germany, as well as
- Morgan, Lewis & Bockius UK LLP, with
  - Registered offices at Condor House, 5-10 St Pauls Churchyard, London EC4M 8AL, and
  - branch offices at 68 rue du Faubourg Saint-Honoré, 75008, Paris, France, and 47 Av. Hoche, 75008, Paris, France

(collectively, the "**Firm**", "**we**", or "**us**") on the collection, use, disclosure, transfer, and other processing of their individually identifiable information ("**Personal Data**"). Under applicable European Union ("**EU**") and United Kingdom ("**UK**") laws, including, but not limited to, the General Data Protection Regulation 2016/679 ("**GDPR**"), the UK Data Protection Act and any supplementing laws and regulations ("**Data Privacy Laws**"), the Firm is a data controller of the Personal Data covered by this Notice.

This Notice is provided in accordance with the Data Privacy Laws and applies only to former, current, and prospective (i) clients of our EU and UK offices, and (ii) clients of our non-European offices who are resident in the European Economic Area ("**EEA**") or the UK where we process their Personal Data (together, "**Clients**"). It identifies the Personal Data that we receive and how we use this information to serve our Clients. This Notice does not apply to other Clients or any residents in any territory other than in the EEA and the UK.

Where the Firm provides legal services to its Clients, we take the position that the Firm is the data controller of the Personal Data that it obtains from its Clients or from other sources in connection with these legal services. The identity of the data controller of the Personal Data that we process will depend on if you are engaging with Morgan, Lewis & Bockius LLP or any of our affiliates. This Notice is intended to fulfil the Firm's obligation to provide information to its Clients whose Personal Data it processes in this capacity. Please also review our [Global Privacy Policy](#), which is incorporated by reference into this Notice.

We also include in this Notice information regarding the Personal Data of third parties that we process in our capacity as a data controller in the course of providing services to our Clients.

### 2. PERSONAL DATA

The Personal Data that we process primarily includes contact information of our Clients and their current or former employees and their other personnel, along with any other

# Morgan Lewis

data relating to such individuals in which they are identified or from which they are identifiable, such as:

- each individual's name, contact information, and information about where he or she works or resides; and
- in rare cases only, to the extent provided to us by a Client or its employees or other personnel:
  - details regarding the individual's health, sickness, and/or disability, and
  - information about the individual's sex life, political opinions, religious or philosophical beliefs, trade union membership, racial or ethnic origin, and/or criminal records.

It also includes Personal Data of third parties in documents and emails that a Client sends to us, such as a third party's name, phone number, address, email address, and other information regarding the issue or matter for which we have been engaged to provide legal services.

We may also collect payment information, such as your credit card or bank account details, and other information such as the date and time of your transaction.

### 3. SOURCES OF PERSONAL DATA

We may obtain Personal Data from the following sources:

- Directly from our Clients or via other information provided to us during the Client's engagement with us;
- Public sources, such as the internet and social media sites; and
- Third parties, including vendors engaged by us or our Clients to provide services on our or our Client's behalf.

### 4. PURPOSES FOR PROCESSING PERSONAL DATA

The Firm processes Personal Data in connection with, and to provide legal services to, our Clients—notably, to facilitate our provision of such services, to respond to queries, and for

other professional dealings with our Clients. The processing of such Personal Data may be a statutory requirement for providing legal services (i.e. for conflict check purposes or to comply with anti-money laundering laws) and we will not be able to provide legal services without the required Personal Data in such cases.

We are also permitted to process Personal Data to comply with our legal and regulatory obligations, our contractual (including pre-contractual) obligations to our Clients to provide the services to them, and for our own legitimate interests.

Where you are the Client, payment information is also necessary for the performance of a contract between you and us, and/or to take steps, at your request, prior to entering into a contract.

Where you are not the Client, the processing of your Personal Data is necessary for our legitimate interests and those of our Clients, namely, administering the legal services.

Based on our legitimate interests and to the extent allowed by applicable law, we may process Personal Data of personnel employed or engaged by our Clients and other contacts for business development and marketing purposes, such as sending LawFlashes and other legal updates, and invitations to seminars, webinars, and other events hosted or sponsored by the Firm. Individuals may unsubscribe from these marketing communications at any time. We will not use this Personal Data for any additional purposes without express consent to do so, unless we have another lawful ground on which to use this information under the Data Privacy Laws.

The Firm may process your Personal Data using (i) cloud services, and (ii) artificial intelligence (including portable models) in a closed, proprietary environment. Such cloud and artificial intelligence services may be hosted in the United States (US), United Kingdom (UK), and/or other countries, including those that do not provide the same level of data protection as the jurisdiction in which you reside. The Firm will exercise due diligence in its selection of these services and will ensure that adequate technical and

organizational security measures are in place to safeguard your Personal Data through use of these services.

We will not process Personal Data for automated decision-making, including profiling.

## 5. DISCLOSURE OF PERSONAL DATA

The following are instances when we may disclose Personal Data to other parties (in or outside your country of residence):

- To comply with the law or respond to compulsory legal processes (such as a search warrant or court order), or in response to a request for information from a regulator or governmental authority, or in the course of actual or anticipated litigation or otherwise for legal purposes, i.e. to other law firms, courts, or government authorities to protect our Clients' rights and/or to provide services to our Clients; and/or
- To protect the rights, property, or safety of the Firm, or any of our respective affiliates, business partners, or Clients, or otherwise in the legitimate business interests of the Firm and/or our affiliates and in accordance with Data Privacy Laws; and/or
- With other law firms, courts, and governmental authorities, to protect the legal rights of our Clients, or in accordance with litigation processes, and to provide our legal services under the agreements with our Clients.
- With another business entity in connection with the sale, assignment, merger, or other transfer of all or a portion of the Firm's business to that business entity. We will require that such recipients undertake to protect this Personal Data as required by the Data Privacy Laws.
- To third parties providing information technology support, technical and organisational services, legal, audit, or other advisors, and other service providers (which may include or involve cloud storage). The Firm will exercise appropriate due diligence in its selection of these providers.

Among other things, the Firm will require that such providers agree, in writing, to maintain adequate technical and organisational security measures to safeguard the Personal Data, process Personal Data only as instructed by the Firm and for no other purposes and comply with the privacy and security standards described in this Notice.

## 6. INTERNATIONAL TRANSFER OF PERSONAL DATA

Due to the global nature of the Firm, some Personal Data is processed by us outside of the EU and UK, including in the United States, China, Japan, Singapore, the United Arab Emirates, Saudi Arabia, Kazakhstan, and Hong Kong, and may be stored within the particular country where the local office is located. The Firm takes appropriate steps to safeguard the privacy and security of all categories of Personal Data as required under the Data Privacy Laws. In these cases, we comply with the requirements for data transfers out of the EU, the EEA and the UK to countries of inadequate data protection and have implemented standard contractual clauses in the form approved by the UK and the European Commission based on risk assessments to the extent required. For our Frankfurt and Munich branch offices, we use the form of a data-protection guarantee. In certain other cases, the Firm may rely on the derogations in Article 49 GDPR for its data transfers out of the EU and UK, such as explicit consent of the data subject or if the transfer is necessary for the establishment, exercise or defense of legal claims.

The Firm's security measures to protect the Personal Data are described below in this Notice. We do not allow any third parties to have access to this Personal Data, except as required or permitted by applicable laws or in accordance with this Notice. We may disclose or allow access to this Personal Data to our subcontractors, agents, legal advisers, auditors, and other relevant business advisers as stated above. Such recipients may be located in countries, including the United States, that do not provide a level of data protection as set forth in the Data Privacy Laws. The UK and Japan are currently deemed by the EU to provide adequate protection. We have taken appropriate steps to

ensure that such entities process the Personal Data in accordance with applicable law.

Please note that our information technology systems, including email, are hosted and all data is stored on servers located in the US.

## **7. LEGAL BASIS FOR PROCESSING PERSONAL DATA**

The Firm's contractual (and pre-contractual) and legal obligations, as well as its legitimate business interests under the Data Privacy Laws, form the legal basis of the processing described in this Notice. The Firm's legitimate interests or those of a third party include our requirements to use Personal Data in litigation, investigations, regulatory or governmental enquiries, or for other legal or regulatory purposes involving the Firm and/or any affiliate of the Firm and may also include the need to transfer your Personal Data to third countries with differing data-protection laws.

## **8. DATA SECURITY**

We understand that storing Personal Data in a secure manner is an essential requirement of the Data Privacy Laws and, therefore, we employ reasonable physical, technical, and organisational security measures to protect Personal Data against foreseeable risks, including accidental, unlawful, or unauthorised use, access, disclosure, destruction, loss or modification, whether it is processed in your local jurisdiction, in the United States or elsewhere. More specifically, our information security team has developed policies, standards, and procedures to support and enforce preventive and detective operational controls to ensure the confidentiality, integrity, and availability of our Client data, such as Log Collection Analysis and Event Correlation, Perimeter Protection, Account Security, Physical Security, User Access, Encryption, Data Loss Prevention, and Vulnerability Management. In addition, Firm personnel are required to read and attest to the Firm's code of business conduct and confidentiality and data security policies on an annual basis. Personnel are also required to attend online data privacy and security training.

Although we make good-faith efforts to store the information we receive from and on behalf of our Clients in a secure operating environment that is not available to the public, we cannot guarantee complete security. Further, while we work to ensure the integrity and security of our network and systems, we cannot guarantee that our security measures will prevent third-party "hackers" from illegally obtaining this information.

## **9. RETENTION, ACCESS, AND ACCURACY OF PERSONAL DATA**

We intend to keep Personal Data accurate and up to date. We retain the Personal Data for the duration of the Client engagement and, depending on the applicable jurisdiction in which a Client is located, for seven or 10 years after the end of the engagement for legal, regulatory, audit, and tax requirements.

Under applicable law, individuals have the right to (each subject to applicable laws):

- inquire whether we process Personal Data about them and to access such data;
- request correction of their Personal Data that is inaccurate;
- obtain information related to the Firm's policies and practices in relation to Personal Data;
- transfer their Personal Data to a third party (data portability);
- request the erasure of their Personal Data; and
- request the restriction of or object for legitimate reasons to the processing of Personal Data concerning them.

To exercise any of these rights, individuals may contact the Morgan Lewis Privacy Office at <mailto:MLPrivacyOffice@morganlewis.com>. The Morgan Lewis Privacy Office serves as the data-protection officer of the Firm under the GDPR. In addition, the Firm has local data-protection officers representing each of its European offices, that may be contacted using the same email address.

# Morgan Lewis

## 10. RIGHT TO RAISE CONCERNS

Individuals have the right to raise concerns to the Firm or to a supervisory authority about the Firm's processing of their Personal Data. If you wish to raise concerns with the Firm, please contact the Morgan Lewis Privacy Office at [MLPrivacyOffice@morganlewis.com](mailto:MLPrivacyOffice@morganlewis.com). The applicable supervisory authority of the Firm is the supervisory authority in the country where the individual is located.

## 11. QUESTIONS

If you have any questions about this Notice or wish to (a) access or review your Personal Data or learn more about who has access to Personal Data, or (b) make another type of request related to Personal Data, please contact the Morgan Lewis Privacy Office at [MLPrivacyOffice@morganlewis.com](mailto:MLPrivacyOffice@morganlewis.com).

## 12. CHANGES TO THE NOTICE

Should we change our Personal Data practices or this Notice, we will issue a revised Notice and/or take other steps to notify you of the changes in accordance with applicable laws.