

# DAVIS POLK & WARDWELL LLP

## DATA PROTECTION POLICY

### Overview

- Davis Polk & Wardwell LLP and its affiliated offices (collectively **Davis Polk** or the **firm**) and their personnel have the responsibility to protect and safeguard the confidentiality of all personal data (**Personal Information**) collected, held or processed by Davis Polk. This Policy, together with the firm's Privacy Policy, applies to all Davis Polk partners, counsel, associates and general staff and sets out Davis Polk's global policy in respect of the rights of individuals with respect to their Personal Information and the responsibilities of partners, counsel, associates, general staff and the firm with respect to access to and use of that Personal Information. Each person working for or representing Davis Polk is personally responsible for maintaining the security and confidentiality of Personal Information in Davis Polk.
- Any Personal Information collected, held or processed by Davis Polk relating to any individual is subject to the relevant provisions of applicable local law. The provisions set out in this Policy are intended to be the firm's global guidelines and are therefore subject to any applicable local law provisions and/or staff policies that may govern the use of Personal Information in each jurisdiction where we have an office. Where there is a conflict between this global policy and a provision of local applicable law and/or Davis Polk policy, the local provision will take precedence.
- There are eight principles for processing Personal Information. The information must be: fairly and lawfully processed; processed for limited purposes and not in any manner incompatible with those purposes; adequate, relevant and not excessive; accurate; not kept for longer than necessary; processed in accordance with the individual's rights; secure; and not transferred to countries without adequate protection.
- These principles apply to all Personal Information collected, held or processed by Davis Polk. They cover the Personal Information of general staff, partners, associates, counsel, contractors, job applicants, clients and even third parties with no direct connection to the firm.
- This Policy applies to Personal Information held in electronic records (for example, on computers, laptops and personal digital assistants used by personnel for work purposes) or in manual filing systems (for example, paper files, rolodexes, microfilm and other media, where that system allows Personal Information about a specific individual to be readily identified).

### Definitions

- **Processing** is broadly defined and includes: obtaining, recording, holding, using, organizing, altering, retrieving, disclosing, erasing or destroying Personal Information.
- **Information or Data** includes, without limitation, information stored in a form capable of being processed electronically, or stored as part of a manual filing system (including index cards or filing cabinets, where that system allows Personal Information about a specific individual to be readily identified).
- **Personal Information** is any personal information or data relating to a living individual and from which that individual is identifiable, including Sensitive Personal Information (where permitted by applicable local law). This may include: name, date of birth, address and title, payroll details, financial details, employment or other references about him/her, a description in information from which the individual

can be identified, biometric and photographic data, and other biographical information about that individual.

- **Sensitive Personal Information**, subject to applicable local law, may include, without limitation, any Personal Information relating to a living individual including: racial or ethnic origin, political opinions, religious beliefs, trade union membership, sexuality, criminal proceedings or convictions and physical or mental health.

The above definitions used in this Policy are for guidance and are not exhaustive and are subject to applicable local law requirements and interpretation at all times.

## **The Rules**

Anyone processing Personal Information must comply with the eight principles of good practice set out below. Personal Information must be:

### **1. Fairly and Lawfully Processed**

The individual must be informed about who will be processing the Personal Information and why the Personal Information is to be processed, in accordance with applicable local law requirements. All practicable steps will be taken to ensure that the individual is informed as to whether the supply/collection of the Personal Information (including sensitive Personal Information) is obligatory or voluntary and where the supply of that Personal Information is obligatory for some specified purpose, the individual will be informed of the consequences of failure to supply that Personal Information.

In addition, particular care must be taken to ensure that the processing of Personal Information does not breach any copyright laws, duty of confidence or any other provision of applicable local law.

#### **1.1 Personal Information**

Personal Information will not be considered to be processed fairly unless certain conditions are met and, subject to applicable local law requirements and permissions, these conditions may include: the individual has consented to the processing; or the processing is permitted by applicable law, or any exemption contained in applicable law justifies the processing, in circumstances where consent is not required; or the processing is necessary for the legitimate interests and/or performance of a contract with the individual (e.g., payroll or obtaining references); or the processing is necessary to comply with any legal obligation; or the processing is necessary for the purposes of a legitimate interest pursued by the firm (unless it could prejudice the individual's interests); or the processing is necessary to carry out public functions; or the processing is necessary to protect the vital interests of the individual.

#### **1.2 Sensitive Personal Information**

Sensitive Personal Information may be processed if permitted by applicable local law (other than in France and Spain), and will not be considered to be processed fairly and lawfully unless processed in compliance with strict conditions of any such applicable local law which may include: the individual has given his/her explicit consent; or the processing is permitted by applicable law, or any exemption contained in applicable law justifies the processing, in circumstances where consent is not required; or the processing is necessary for the firm to meet a legal obligation in relation to employment (e.g., maintaining equal opportunity records); or the processing is necessary to protect the vital interests of the individual; or the processing is necessary for the administration of

justice or legal proceedings. The firm collects Personal Information relating to individuals (including general staff, partners, associates, counsel, contractors, job applicants, clients and third parties) from a variety of sources but mainly from the individuals themselves.

- 1.3 Davis Polk carries out both routine and specific monitoring (where the circumstances warrant such action). Personal Information may therefore be collected directly or indirectly from such monitoring and/or from monitoring devices or by other means (for example, door access control mechanisms, closed circuit television, telephone logs, recordings and email and Internet logs). In these circumstances, the Personal Information may be processed, for example, for regulatory, legal, compliance or billing purposes or where the firm is investigating possible abuse of firm systems, or potential civil or criminal offences. Where Davis Polk carries out such monitoring it will, wherever reasonably practicable, endeavor to protect obviously private files.

## **1. Processed for Limited Purposes**

- 1.1 Personal Information should only be processed for specific and lawful purposes, each of which has been disclosed to the individual; or is obvious in the context in which the Personal Information is collected; or is permitted by applicable law. The Personal Information should not be processed in any manner incompatible with the stated purposes.
- 1.2 Personal Information (including Sensitive Personal Information) relating to employees is collected (including via electronic communications) for several business purposes including, without limitation: for the firm's administration and management of its business; for compliance with applicable procedures, laws and regulations; for the transfer, storage and processing of Personal Information by the firm (or its agent(s) including any third parties retained by it together with their successors and assigns); the firm's administration and management of its employees (including without limitation for: taxation and wage administration; medical information for the administration of private medical and other insurance schemes; performance evaluations; contingency planning; business travel; training; career planning; recruitment; provision of references; reimbursement of expenses; disciplinary purposes; compiling personnel profiles, contact lists and directories); and any matters ancillary to the aforesaid.
- 1.3 Personal Information collected by Davis Polk may also be shared with other Davis Polk offices in various jurisdictions (information on our offices can be obtained at <https://www.davispolk.com/offices>) for the same purposes as set out in 2.2 above and in Article 3 of our Privacy Policy. The Davis Polk office which collects such Personal Information is the responsible party to administer and manage such Personal Information although it may transfer Personal Information to other offices as set out in Section 8 below.
- 1.4 As a matter of firm practice, all channels through which Personal Information is gathered (for example, via application forms, the Davis Polk website, etc.) will normally contain wording and/or a reference to the firm's Privacy or Data Protection Policies so that individuals are informed of the intended use of the Personal Information being collected. Any email or fax will normally contain standard notification wording in the template or footer which directs individuals to the firm's "Disclaimer" which includes its Privacy Policy. The templates will also ask unintended recipients immediately to delete any email or fax received in error and copies of such communications should always be retained until it is envisaged that there will be no further contact with the individual concerned.
- 1.5 It is Davis Polk's policy not to share any Personal Information with any non-affiliated third parties (information on our offices can be obtained at <https://www.davispolk.com/offices>) unless: Davis Polk is so directed by or with the consent of the individual in question; it is necessary in the processing or administration of transactions/cases; it is in connection with providing services; it is

related to Davis Polk's operations; or it is permitted by applicable law or any exemption contained in applicable law.

Under no circumstances, unless prior authorization is obtained from the individual, will any Personal Information be disclosed to non-affiliated third parties other than as further described herein. Equally, Personal Information should only be disclosed within Davis Polk on a "need-to-know" basis.

Personal Information may be shared with other non-affiliated third parties where such third party entity (and/or its successors and assigns) is performing certain services on behalf of Davis Polk, pursuant to its direction, or as directed or consented by the individual, such as auditors, technical service providers or other service providers that require the processing of Personal Information, for: the specified purposes as set out in this Policy, as may be permitted or required by law, as provided for by any contractual arrangement, and in connection with Davis Polk's business and its operations (including where disclosure is necessary in order to facilitate the conduct of the specific matter including transactions/cases). In such circumstances, we will inform or notify you in advance of us disclosing your Personal Information to that third party, unless it is not possible to do so or would involve disproportionate effort and which might not be technically or commercially feasible in all the circumstances.

- 1.6 Davis Polk may also disclose Personal Information to government, law enforcement or regulatory authorities or as otherwise required or permitted by applicable law and if Davis Polk is contacted by any such authority, Davis Polk may be required to provide any requested Personal Information to the extent so required and as provided by law. Any such request received by a partner, counsel, associate or general staff should be referred to the Data Protection Partner and no Personal Information should be disclosed in this way without the consent of the Data Protection Partner.
- 1.7 Where required by applicable law in any jurisdiction, the firm will comply with all necessary authorization and registration requirements, including stipulating the purposes for which it intends to use Personal Information collected during its operations. Register entries will be kept up to date. Please check with the firm's Data Protection Partner if you need to know whether our registration covers your planned processing.

## **2. Adequate, Relevant and Not Excessive**

- 2.1 Personal Information held should be sufficient for the stated purposes but not more than sufficient for those purposes. Periodic audits will be carried out to ensure that no irrelevant or excessive information is held.

## **3. Accurate**

- 3.1 Any Personal Information stored must be accurate and up to date. Periodic audits will be conducted to check Personal Information for accuracy and to ensure that out of date material is updated or discarded. The interval for such audits will be determined by reference to the nature of the Personal Information and the purpose for which it is being held or processed, including any legal or regulatory requirements to retain the Personal Information. This should be achieved by regularly reviewing Personal Information held to ensure compliance with applicable legal, operational and regulatory requirements.
- 3.2 Davis Polk will send annual reminders to its employees to remind them to update their Personal Information. All individuals should ensure that they notify Davis Polk of any material changes to their key Personal Information such as home address, name, emergency contacts, etc.

#### **4. Not Kept Longer Than Necessary**

- 4.1 Personal Information held by the firm for a specific purpose must not be held for longer than is necessary for that purpose and procedures should be in place to allow selective deletion of information. If during any periodic review, it is discovered that the purposes for which the Personal Information was gathered are no longer necessary purposes, i.e., the Personal Information is no longer in use (or relevant) and there is no legitimate reason for the personal information to be retained, the Personal Information must be destroyed.
- 4.2 All Personal Information should be disposed of at the end of any retention period that is required or permitted by applicable law, in a manner appropriate to its sensitivity. All back-up and archive copies should also be destroyed.

#### **5. Processed in Accordance with the Individual's Rights**

- 5.1 Subject to the provisions of applicable law from time to time, individuals may be entitled to exercise certain individual rights provided for under local data protection laws. These may include: a right of access to, correction or deletion of Personal Information. Davis Polk recognizes that if individual rights exist and an individual makes a request to exercise such a right it will comply with its legal obligations in that regard. Any counsel, associate or general staff wishing to exercise any such right should contact their Office Manager or the Firm's Director of Human Resources (partners and other individuals should contact the Data Protection Partner). Individual rights are discussed further in Section 9 below.

#### **6. Security**

- 6.1 Appropriate security measures are taken by Davis Polk to safeguard Personal Information against any accident, loss, destruction, damage and unauthorized or unlawful processing. Such measures include, but are not limited to, access controls (e.g., individual passwords), audits and training for personnel responsible for processing, maintaining and transferring personal data. Personnel are regularly reminded of these responsibilities. Disciplinary rules are in place should there be a breach of duties and responsibilities. Additional security measures are in place for Sensitive Personal Information (as may be required by applicable law) which ensure that access is on a strict "need to know" basis.
- 6.2 Any personnel handling Personal Information are required to maintain, secure and protect the confidentiality of such information and take all necessary precautions to protect Personal Information from any unauthorized use, disclosure or potential loss. Measures that are undertaken to secure Personal Information include, but are not limited to, the following: all personnel must at all times comply with Davis Polk's IT Security Policy; access to electronic databases or documents containing Personal Information is only provided to those personnel who have work-related reasons for access; records containing Personal Information are stored in a secure location. Electronic databases and documents are safeguarded by password protection and/or other access-limiting methods. Passwords are changed periodically. Personal Digital Assistants (e.g., BlackBerrys) that may contain Personal Information are password protected. Computers with access to Personal Information are not to be left unattended, unless they are password protected through screen savers; when an individual is no longer employed by Davis Polk, his/her access to Davis Polk's computer systems will immediately be terminated; all computers are protected with multi-tier anti-virus software. Computer systems are archived and backed up periodically; any Personal Information not maintained electronically is maintained in a locked file cabinet or other secure location when not in use; and additional security measures are in place for Sensitive Personal Information (as provided for by applicable legislation) to ensure that access is on a strict "need to know" basis only and it is secured even when being left unattended for a short while.

- 6.3 Furthermore, personnel are subject to all restrictions, provisions and covenants contained in any confidentiality, non-solicitation and non-competition agreement(s) and acknowledgment(s) executed in connection with their employment and any rules and policies implemented by Davis Polk. Under no circumstances shall personnel use Personal Information for their own personal use or otherwise outside of their employment with Davis Polk.

## **7. Not Transferred to Countries Without Adequate Protection**

- 7.1 Davis Polk is an international firm and our headquarters are in the United States of America. In order to operate our business, we may need to transfer Personal Information to locations outside the local jurisdiction in which partners and Davis Polk employees are based and process Personal Information outside that jurisdiction. Personal Information may therefore be controlled and processed by any of Davis Polk's offices, some of which are outside the European Economic Area (EEA).
- 7.2 Data protection and privacy laws in other jurisdictions may not provide for the same level of protection of your Personal Information as exists in your home country or in the EEA. Personal Information is not to be transferred outside of the EEA except in compliance with certain safeguards and requirements established by applicable law from time to time.
- 7.3 To ensure a sufficient level of Personal Information protection, Davis Polk and its offices have entered into a Global Co-Operation Agreement containing the model clauses as recommended by the European Commission, to ensure that Personal Information transferred between Davis Polk offices will be dealt with in accordance with applicable law and ensuring sufficient protection of transferred Personal Information. For the purposes of our Paris office, the CNIL authorised the transfer of Personal Information pursuant to decision No. 2009-558 of 24 September 2009. For the purposes of our Madrid office, the AEPD authorized the transfer of Personal Information pursuant to decisions TI/00160/2009 and TI/00161/2009 of 12 March 2010.
- 7.4 In respect of Personal Information which falls outside of or is not covered by the Global Co-Operation Agreement, Personal Information should not be transferred from within the EEA to any person or organization outside of the EEA by any means (including, for example, by such methods as email or through any intranet or other computer network), unless: the individual to whom the Personal Information relates has given his/her consent to the transfer; or the processing is permitted by applicable law, or any exemption contained in applicable law justifies the processing, in circumstances where consent is not required; or that country or territory enforces an adequate level of protection for the rights and freedoms of individuals in relation to the processing of Personal Information; or should that country or territory not offer the same level of protection for the rights and freedoms of individuals in relation to the processing of Personal Information, the transfer has been authorized by a relevant national authority.

## **8. Individual Rights**

- 8.1 An individual may have certain rights with regard to his/her Personal Information conferred by applicable local law. These rights may include: rights of access to Personal Information held about him/her; and to have such information either corrected or erased. Subject to its legal obligations in each jurisdiction and to the application of any legal exemptions, Davis Polk will comply with any such individual rights. Any counsel, associate or general staff wishing to exercise any such right should contact their Office Manager; partners and other individuals should contact the Data Protection Partner.

### ***Access Rights***

- 8.2 Under applicable law, individuals may be entitled to make a formal request to access certain of their Personal Information which is held by Davis Polk. Where applicable law confers such a right on an individual, Davis Polk will comply with any such request provided that the individual meets the requirements within the relevant time periods provided. Any such request should be made to the Office Administrator in the individual's office or Data Protection Partner (as appropriate) who will be able to provide more details about rights of access in the relevant office concerned.
- 8.3 Any such request for access to Personal Information must comply with any applicable legal requirements and should be in writing and accompanied by the following information: reasonable information as to the individual's identity, any other information required and payment of any fee, that may be permitted by applicable law; the individual's contact details, and the date and signature; and any other information required to comply with any other access conditions/requirements under applicable law.
- 8.4 Applicable law may provide circumstances and/or categories of Personal Information which may not be or are not required to be disclosed by Davis Polk under such an access request. In such circumstances, Davis Polk will comply with its legal obligations and will notify the individual if any information requested cannot be provided. Davis Polk will only provide access if permitted by applicable law, including obtaining any relevant consent.

### ***Rights to Amend/Delete Personal Information***

- 8.5 Subject to the provisions of applicable local law, individuals may also have certain of the following rights in relation to their Personal Information: a right to object to processing (on grounds provided for under applicable local law); a right to prevent processing for direct marketing; a right to object to decisions being taken by automated means; a right to have inaccurate Personal Information corrected; a right to stop unauthorized transfer to a third party; or a right to have Personal Information corrected, blocked, erased or destroyed.
- 8.6 If there is any confusion, complaint or doubt about any aspect of information processing or individual rights in your jurisdiction, your questions should be directed to your Office Manager or the Data Protection Partner.

## **9. Compliance with this Policy and Unauthorized Use or Disclosure**

- 9.1 Processing of Personal Information outside these guidelines is not permitted by Davis Polk. If a partner, counsel, associate, or general staff unlawfully obtains, discloses or sells any Personal Information collected, held or processed by, or on behalf of, the firm without consent, he or she may be guilty of a criminal offence. Anyone violating this Policy may be subject to disciplinary action, up to and including dismissal (where appropriate). If in doubt, please contact Davis Polk's Data Protection Partner Leo Borchardt at [leo.borchardt@davispolk.com](mailto:leo.borchardt@davispolk.com).
- 9.2 Anyone who has knowledge of unauthorized access, use or disclosure of Personal Information should immediately report it to the Data Protection Partner. Unauthorized access, use or disclosure of Personal Information or failure to report such unauthorized access, use or disclosure, will result in appropriate disciplinary action, which may include the termination of employment.