|  |
| --- |
| **[COMPANY NAME]** |

**[COMPANY]**

**Internal**

**DATA protection policy**

**Contents**

[1 Policy statement 3](#_Toc46920227)

[2 Compliance and Administration 3](#_Toc46920228)

[3 Definitions 4](#_Toc46920229)

[4 Data collection and protection principles 4](#_Toc46920230)

[5 Disclosure and sharing of Personal Data 8](#_Toc46920231)

[6 Dealing with Data Subjects’ rights and requests 9](#_Toc46920232)

[7 Questions about this Policy 9](#_Toc46920233)

# Policy statement

## The COMPANY (“COMPANY”) and/or its subsidiaries and affiliates, including [LIST AFFILIATES] (collectively [name], “we” or “us”) are committed to safeguarding the privacy of the Personal Data that we gather.

## The [COMPANY] Internal Data Protection Policy applies to Personal Data and to the management of that Personal Data in any form – whether oral, electronic or written.

## This policy gives effect to [COMPANY]’s commitment to protect any Personal Data, including that of its employees and third parties, and has been adopted by [COMPANY LEADERSHIP? BOARD?] as well as all its subsidiaries, affiliates and related entities. “Personal Data”, further defined below, for the purposes of this policy includes individuals’ names, dates of birth and other personal information from which they can be identified.

## This policy and any other documents referred to in it sets out the lawful bases on which we will process Personal Data we collect from any Data Subjects, or that is provided to us by Data Subjects or other sources. It sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store Personal Data.

## This policy may be amended at any time, regardless of employees’ contractual terms.

# Compliance and Administration

## Our clients and employees have rights with regard to the way in which their Personal Data is collected, stored and processed. We recognise that the fair and lawful treatment of this Data will maintain confidence in [COMPANY] and will support successful operations.

## All [COMPANY] employees and contractors must comply with this policy when processing Personal Data on [COMPANY]’s behalf. Any breach of this policy may result in disciplinary action.

## The Personal Data, which we hold in relation to our customers, employees, suppliers and other third parties is subject to certain legal safeguards specified in applicable data protection laws and regulations, including the Data Protection Law, DIFC Law No. 5 of 2020 (“DIFC DP Law 2020” and collectively, the “Applicable Laws”).

## The [COMPANY] has taken the following steps:

### established a compliance program; and

### appointed a Data Protection Officer, who must act independently, reporting to senior management, and who is responsible for:

* + 1. ensuring compliance with the DP Law 2020 and all Applicable Laws and with this policy;
    2. ensuring the DP Notification in the DIFC Client Portal is updated on an annual basis as well, in accordance with [applicable procedures to do so];
    3. providing training for staff about data protection;
    4. conduct data protection impact assessments and risk analysis;
    5. supporting [COMPANY] in keeping and updating a register of processing activities; and
    6. ensuring compliance with any other requirements necessary to comply with the DP Law 2020 and all Applicable Laws.

## Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to [ROLE – DPO?], who can be reached at [EMAIL ADDRESS, TELEPHONE, ETC]

# Definitions

## Data is information which is processed i) by means of equipment operating automatically in response to instructions given for that purpose, or ii) on paper or as part of a paper-based filing systems intended for processing electronically.

## Data Subjects for the purpose of this policy include all living individuals about whom we hold Personal Data. All Data Subjects have legal rights in relation to their Personal Data.

## Controllers are the people who or organisations which determine the purposes for which, and the manner in which, any Personal Data is processed. They are responsible for establishing practices and policies in line with the Applicable Laws. We are the Controller of all Personal Data used for commercial or other notified purposes.

## Processors include any person or organisation that is not a Data user that processes Personal Data on our behalf and on our instructions. Employees of Controllers are excluded from this definition but it could include suppliers that handle Personal Data on [COMPANY]’s behalf.

## Personal Data means Data relating to a living individual who can be identified from that Data (or from that Data and other information in our possession). Personal Data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

## Processing is any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. Processing also includes transferring Personal Data to third parties.

## Special Categories of Personal Data is information revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life. Special Category Data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

# Data collection and protection principles

## [COMPANY] may in the ordinary course of business collect and process information about anyone who:

## is employed by us, including contractors and temporary employees;

## uses our mobile applications, websites, call-centres or other digital interfaces;

## attends our business development, marketing or other [COMPANY] sponsored events;

## contacts us for information about registering a business in the [COMPANY] or for information about other products and services;

## interacts and communicates with us in a business capacity; and

## provides or handles information relating to suppliers and other third parties.

## Such information may include, but is not limited to:

## Name, gender, home address, and telephone number, date of birth, marital status, emergency contacts;

## Residency and visa status, nationality and passport information;

## Emirates ID number, banking details;

## Information required to comply with laws, the requests and directions of law enforcement authorities or court orders (i.e. debt payment information);

## Information captured on security systems, including CCTV and key card entry systems;

## Voicemails, emails, correspondence and other work product and communications created, stored and transmitted by an employee using [COMPANY]’s computer or communications equipment;

## Employee information, including:

## Sick pay, pensions, insurance and other benefits information (including the gender, age, nationality and passport information for spouse, minor children or other eligible dependents and beneficiaries);

## Dates of hire, date(s) of promotion(s), work history, technical skills, educational background, professional certifications and registrations, language capabilities, training courses attended;

## Records of work absences, vacation entitlement and requests, salary history and expectations, performance appraisals, letters of appreciation and commendation, and disciplinary and grievance procedures (including monitoring compliance with and enforcing [COMPANY] policies);

## Where permitted by law and proportionate in view of the function to be carried out by an employee or perspective employee, the results of credit and criminal background checks, health certifications;

## Date of resignation or termination, reason for resignation or termination of employment ((i.e. references).

## Anyone processing such information must adhere to the following principles of lawfulness, transparency and accountability:

### Personal Data must be processed lawfully, fairly, and in a transparent manner in relation to the Data Subject.

### Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

### Personal Data must be adequate, relevant and limited to those which are necessary in relation to the purposes for which they are processed.

### Personal Data must be accurate and, where necessary, kept up to date.

### Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed.

### Personal Data must be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

### The Controller shall be responsible for and be able to demonstrate compliance with these principles.

## Fair processing

### The Applicable Laws are not intended to prevent the processing of Personal Data, but to ensure that it is done fairly and without adversely affecting the rights of the Data Subject.

### For Personal Data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the Applicable Laws. These include, among other things, the Data Subject's consent to the processing, or that the processing is necessary for the performance of a contract with the Data Subject, for the compliance with a legal obligation to which the Controller is subject, or for the legitimate interest of the Controller or the party to whom the Data is disclosed. When Special Category is being processed, additional conditions must be met.

### When processing Personal Data as Controllers in the course of our business, the [COMPANY] and its employees will ensure that those requirements are met.

### In the absence of any other applicable basis for fair and lawful processing of Personal Data, [COMPANY] processes Personal Data on the basis that the processing is necessary for the purposes of pursuing the [COMPANY]’s legitimate interests or those pursued by a third party or parties to whom the Personal Data is disclosed, except where such interests are overridden by compelling legitimate interests of the Data Subject relating to the Data Subject's particular situation

## Processing for limited purposes

### In the course of our business, we may collect and process Personal Data. This may include Data we receive directly from a Data Subject and Data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

### We will only process Personal Data for specific purposes or for any other purposes specifically permitted by the Applicable Laws. We will notify those purposes to the Data Subject.

## Adequate, relevant and non-excessive processing

### We will only collect Personal Data to the extent that it is required for the specific purpose notified to the Data Subject.

## Accurate, Complete and Up-to-Date Data

### We will ensure that Personal Data we hold is accurate and kept up to date. We will take reasonable steps to destroy or amend inaccurate or out-of-date Data.

## Timely processing

### We will not keep Personal Data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all Data which is no longer required or which a Data Subject has asked that we destroy or modify.

### We will conduct timely reviews of our processing operations with respect to Data that is collected and stored in our systems. Such reviews will include but are not limited to understanding where our Data is processed, who our sub-processors are (if any) and any recipients of our Data and the purposes for which they are processing it, if such information may legally be made available to us.

### We will to the extent required by law comply with any statutory retention periods.

### Where the basis for processing changes for any reason, processes are in place for ensuring one of the following actions is taken with respect to the Personal Data:

* + 1. securely and permanently deleted;
    2. anonymised so that the data is no longer Personal Data and no Data Subject can be identified from the data including where the data is lost, damaged or accidentally released;
    3. pseudonymised;
    4. securely encrypted; or
    5. properly archived / put beyond further use.

## Data security

### We will take appropriate security measures against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data.

### We will put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Personal Data will only be transferred to a Processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

### All [COMPANY] employees are responsible for ensuring the security of our systems by adhering to this and related policies including the [COMPANY] IT and Security policies, which contain details about your appropriate use and security of the devices and systems that are in the [COMPANY] IT environment.

### We implement as part of our security policies and processes an incident management policy in order to address personal data breaches and how to manage / report them in accordance with Articles 41 (and where required, Article 42 of the DP Law 2020)

## Transferring Personal Data

### We may transfer any Personal Data we hold to and from the jurisdiction in which it is collected. In relation to Personal Data that i) we transfer out of the DIFC or ii) specifically to the UK, the EU or a country within the European Economic Area ("EEA"), we may subsequently transfer that Personal Data to another country provided that one of the following conditions applies:

* + 1. One of the appropriate safeguards is in place under Article 27(2) of the DIFC DP Law 2020.
    2. The country to which the Personal Data are transferred ensures an adequate level of protection for the Data Subjects' rights and freedoms.
    3. The Data Subject has given his consent.
    4. The transfer is necessary for one of the reasons set out in the Applicable Laws, including the performance of a contract between us and the Data Subject, or to protect the vital interests of the Data Subject.
    5. The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
    6. The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the Data Subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

## Accountability to Data Subjects

### Our use or disclosure of Personal Data must be necessary for the purpose(s) or compatible with the purpose(s) for which we collect and keep the Data. Except in certain limited circumstances (including where we are required by law) we should only use and disclose the Data in ways consistent with such purpose(s).

### We will inform through publicly available privacy notices (i.e., on our corporate website) Data Subjects who provide us with or inform us about their Personal Data regarding:

* + 1. The purpose or purposes for which we intend to process that Personal Data
    2. How we process their Personal Data, including information about third party suppliers who process it on our behalf.
    3. The types of third parties, if any, with which we will share or to which we will disclose their Personal Data.
    4. The means, if any, with which Data Subjects can limit our use and disclosure of their Personal Data.
    5. Any other rights they have with respect to our use of their Personal Data in line with Applicable Laws.
    6. The methods and mechanisms we have in place to be transparent with and accountable to the Data Subject.
    7. The [COMPANY]’s role as a Controller of their Personal Data and how to reach the Commissioner of Data Protection.

# Disclosure and sharing of Personal Data

## We may share Personal Data we hold with any member of our group, but must do so confidentially in all instances.

## We may also disclose Personal Data we hold to third parties:

* + 1. In the event that we sell or buy any business or assets, in which case we may disclose Personal Data we hold to the prospective seller or buyer of such business or assets.
    2. If we or substantially all of our assets are acquired by a third party, in which case Personal Data we hold will be one of the transferred assets.
    3. If we are under a duty to disclose or share a Data Subject's Personal Data in order to comply with any legal obligation, or in order to enforce or apply any contract with the Data Subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

## We may share Personal Data we hold with selected third parties for the purposes including but not limited to fulfilling employee contract requirements such as payroll and medical insurance; enabling vendors to satisfy Client requirements; or to support relevant Client or employee engagements.

# Dealing with Data Subjects’ rights and requests

## With some limited exceptions, any Data Subjects are entitled to:

* + 1. Request access to any Personal Data that [COMPANY] holds about them (known as a subject access request);
    2. Request that we stop processing their Personal Data, including automated processing of personal data;
    3. Request that we rectify, block or erase any Personal Data we hold about them; or
    4. Make a complaint to the Commissioner of Data Protection regarding the processing of their Personal Data.

## Data Subjects should make the request by writing to the Commissioner of Data Protection or his delegate. Alternatively, the [COMPANY] website contains the [online data protection policy] that provides a link where they will find an explanation of how they may make such requests.

## Anybody at [COMPANY] who receives a written or verbal request or complaint from a Data Subject should immediately engage the procedure set out in the Dealing with Data Subjects’ Rights Policy (available on SAP in the Legal Affairs documents link), as a specific time limit applies to such requests and a breach of the Applicable Laws may occur if [COMPANY] does not respond accordingly.

# Questions about this Policy

## If you have any questions about this Policy, or any concerns or complaints with regard to the administration of this policy, or if you would like to submit a request as described in Section 6 above for access to the Personal Data that we maintain about you, please contact us by any of the following means:

### For current [COMPANY] employees, by contacting your line manager or your HR Business Partner; and

### For applicants and former [COMPANY] employees, by contacting Head of Human Resources.

## Complaints or further escalation at the employee’s option, can be made to the Head of Human Resources and finally to the Commissioner of Data Protection at DIFC.