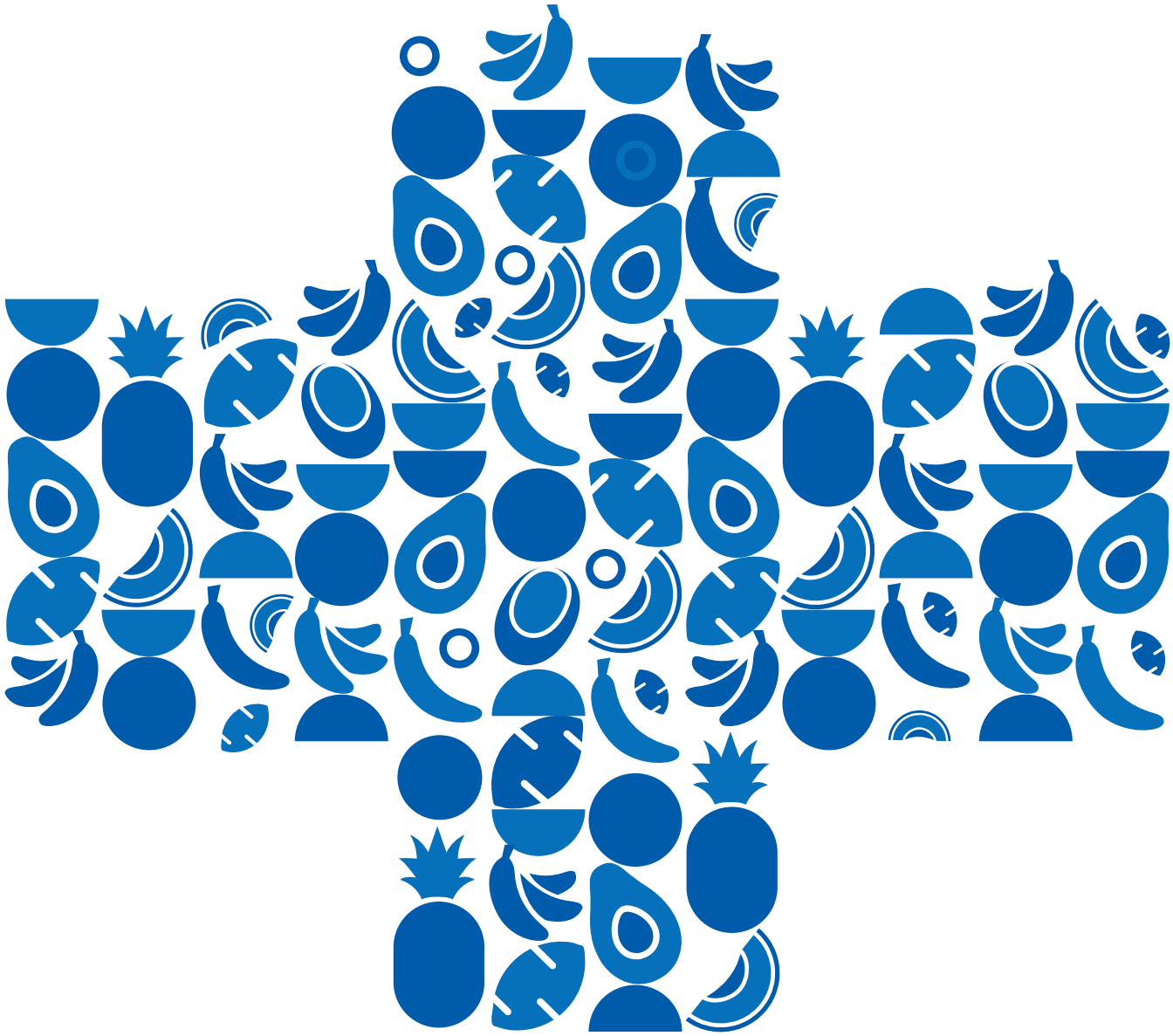
Fyffes Group Data Privacy Policy



Policy in Practice Series: January 2023

TABLE OF CONTENTS

I. SCOPE

Each individual has the right to be informed and make decisions about the collection and other processing of their personal data[1]. This right is provided for by an increasing number of data protection and privacy laws in Europe and around the world, including the Swiss Data Protection Act and the revised Swiss Data Protection Act (together **Swiss DPA**), the EU General Data Protection Regulation (**GDPR**), country-specific laws in the European Economic Area member states (all laws together the **Data Protection Laws**).

This Group Data Privacy Policy (the **Policy**) provides how Fyffes International S.A. and its affiliates as identified on https://www.fyffes.com (the **Group**) will protect such rights and comply with such Data Protection Laws. The Policy shall be complied with by all employees (which term shall also include all contractors and other individuals working within the Group, such as consultants pursuant to Article 29 GDPR) when processing personal data for or at the Group. Of course, if stricter local laws or binding works council agreements apply, they shall take precedence over this Policy.

It is the responsibility of the management of each entity of the Group to take the necessary steps to implement at such Group entity this Policy and any stricter local laws that apply.

Further details on the Group entities' procedures and processes to comply with this Policy and related Data Protection Laws are provided in instructions and manuals which are available on the Group entities' intranet and upon request from the DPC.

II. HANDLING PERSONAL DATA[2]

Data protection is about **Personal Data**, which is any information related to an identified or identifiable individual – also referred to as a **data subject**. It is sufficient that the data subject to whom a set of information relates can only be identified indirectly by using secondary sources (such as an Internet search or another database). Data subjects can be employees, customers, and other people. Anything we do with this personal data, such as collecting, using, storing, disclosing, or deleting personal data, is referred to as **processing**. For certain **special categories of personal data**, Data Protection Laws provide for stricter rules. These special categories of personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for secure identification purposes, data concerning health or the sex life or sexual orientation of a person; under the Swiss DPA, it also includes data on administrative or criminal proceedings and sanctions, data on social security measures and data on the intimate sphere in general.

III. RULES

A. Basic Principles

1. We process personal data in compliance with data protection principles and, where the GDPR applies, only if we have sufficient legal ground, but we avoid relying on consent.

To the extent the processing of personal data is only subject to the Swiss DPA: We will not need a legal ground to process personal data, as long as we comply with the processing principles set out in this Section III. However, legal ground is needed for processing personal data in three specific situations, namely if (i) we fail to comply with one of the processing principles set out in this Section III; (ii) the data subject has expressly objected to the processing at issue, or (iii) sensitive personal data is disclosed to a third party.

If the processing of personal data is subject to the GDPR: Each Group entity is required to only process personal data if there is sufficient legal ground to do so. Hence, all **Data Activity Owners** (as defined in Exhibit A) are required to take appropriate steps to confirm that sufficient legal ground exists by consulting with the **Data Protection Coordinator**/Data Protection Officer (collectively referred to as **DPC**) of the relevant Group entity. The DPC of the relevant Group entity will assist with the determination of the applicable Data Protection Laws. The legal grounds most commonly relied upon for processing personal data under the Swiss DPA and the GDPR include: (i) the performance of a contract with the data subject or the steps taken to enter into a contract with the data subject upon their request; (ii) compliance with a legal obligation; (iii) the data subject's consent, and (iv) an overriding "legitimate interest".

There are a number of other possible legal grounds, and whenever special categories of personal data or criminal data are processed by a Group entity, separate legal grounds must be established in consultation with the DPC of the relevant Group entity in these cases.

[1] For the purposes of this Group Data Privacy Policy, it has been chosen to use "they", "them" and "their" when referring to an individual to use non-binary terms and include all genders.
[2] For the purposes of this Fyffes Group Data Privacy Policy, Personal Data is any information that relates to an identified or identifiable living individual. Different pieces of information collected together can lead to the identification of a particular person also constitute Personal Data. Examples of Personal Data: (i) a name and surname; (ii) a home address; (iii) an email address such as name.surname@company.com; (iv) an identification card number; (v) location data (for example the location data function on a mobile phone); (vi) an Internet Protocol (IP) address; (vii) a cookie ID; and (viii) the advertising identifier of your phone.

Also, the legal grounds must be documented by the Data Activity Owner. In cases where the Data Activity Owner, in consultation with the DPC has determined that an overriding "legitimate interest" is the legal basis, the reasoning and the balancing of the various interests must be documented in writing.

As a general rule, relying on consent should be avoided because it is very difficult to obtain legally valid consent and consent can be withdrawn at any time, without providing any reasons (which means that the Group entity may have to stop processing the personal data if the Group entity relied on consent in the first place). Any employee, in particular the Data Activity Owner, will contact the DPC if consent shall serve as the legal basis.

If personal data from an existing data collection shall be used for another purpose than that for which it was collected for, the Data Activity Owner will contact the DPC to check whether it is permitted.

2. We are transparent and fair when processing personal data.

We will inform the data subject that we are processing their personal data, by telling them, posting notices, using information signs or other means. We will not collect personal data covertly and we will not process it in an unexpected manner for the data subject.

The Data Activity Owner is required to ensure that appropriate privacy notices are made available to the data subjects on our websites and by other appropriate means to tell them more about what the Group entity does with their data. The applicable Data Protection Laws define the information that must be included in these statements. The Data Activity Owner shall consult with the DPC to determine and develop the appropriate privacy notices. The Data Activity Owner, in consultation with the DPC, shall verify whether any new processing of personal data is already covered by an existing privacy notice that has already been made available to the data subjects. When assessing whether the privacy notice covers our newly planned processing activity, the Data Activity Owner will bear in mind that co-workers can also be data subjects (and not only outsiders). Data Activity Owners are required to ensure that personal data is not processed in a manner that could be perceived as unfair or against good faith.

3. We will only use personal data for the purposes for which we collected it.

If a Data Activity Owner plans a new processing activity, the Data Activity Owner needs to understand from the beginning the purposes for which the personal data will be collected and processed. The Data Activity Owner is required to ensure that such purposes are communicated to the data subject concerned at the time of data collection (unless an exception applies). This includes informing the data subject of the disclosure of their personal data to a third party for its own purpose (as a controller), if this is the plan, and any other aspects that must be disclosed by law to the data subject as provided in section 2 above. The Data Activity Owner shall consult with the DPC to comply with this principle.

If the Data Activity Owner wants to use personal data for another purpose than the initial purpose, the Data Activity Owner will contact the DPC of the relevant Group entity to find out whether this is permitted and whether any further steps, such as providing new information to the data subject or consent, is required.

4. We will only collect the data we really need.

We will not try to collect as much personal data as possible, but rather try to limit ourselves to what we really need for the specific purpose. Data Activity Owners are required to comply with this principle.

If a Data Activity Owner wants to gather useful, but not strictly necessary personal data, the Data Activity Owner will contact the DPC. The Data Activity Owner shall try to avoid processing activities that, because of the extent of the gathered data or the extent to which it is used, would make the data subject feel uneasy or concerned or cause reputational damage.

5. We will only keep data for as long as we need it and limit access to it.

We will limit access to personal to those who really need to have access to it ("need to know" basis) and limit it continuously. All employees, in particular Data Activity Owners, are required to take steps to comply with this principle. All employees shall consult the Group's Data Retention Policy[3] for detailed instructions about the retention periods of the various categories of documents kept by the Group entity. If the personal data is no longer needed for the purposes for which it was obtained, and if any legal obligations and legitimate business interests permit, Data Activity Owners shall

[3] To be released soon.

ensure that the data is deleted or anonymized. Data Activity owners shall contact the DPC for instructions on how to do this. When designing a project involving the processing of personal data, the Data Activity Owner shall verify the ability to delete (or properly anonymize) the personal data once it is no longer needed. The Data Activity Owner shall take into consideration from the beginning (e.g. in a project) how to ensure that the data is deleted at the right time and that the right time is not missed.

6. Where reasonably possible, we give data subjects a choice.

This applies even where we do not rely on consent. For example, if a data subject objects to our processing of their data, we will determine whether we are required to stop doing so and, if there are no compelling legitimate grounds and no applicable legal requirements permit so, we will do so. If an employee receives such an objection, they shall consult with the DPC to determine the appropriate handling of such objection. If certain data is not necessary to achieve the intended purposes, the Data Activity Owner shall ensure that the data subjects are aware of their choice whether they want to share it with the Group entity. If a data subject no longer wants the Group entity to use their data for marketing purposes, the Group entity is required to stop such processing. When designing a processing activity involving the processing of personal data, the Data Activity Owner shall ensure that the processing of personal data given voluntarily can be stopped at any time, without great effort.

7. We ensure the accuracy of the personal data we process.

We take reasonable steps to ensure that the personal data is accurate and, where necessary, kept up to date in view of its relevance and purposes. Accordingly, the Data Activity Owner shall take reasonable steps to rectify data or, if that is not feasible, to give it up, and to keep the data synchronized across the board. The Data Activity Owner shall take reasonable steps to ensure that rectifications that were reported to the Group entity (e.g. by a data subject) will "survive" the event of data restoration through a backup.

8. We will pseudonymize and not reidentify data subjects.

Whenever possible, the Data Activity Owner shall ensure that personal data is "coded" in such a manner that the data subjects cannot be identified by those who do not have the "re-identification key" to the code. Data Activity Owner shall take steps to limit access to the code to those persons who need to have access to it. Also, employees will not try to re-identify the individuals to whom pieces of information relate, unless they have a good reason to do so. Both measures will help to protect their privacy.

9. We will have adequate data security in place, technically and otherwise.

It is important that the confidentiality, integrity and availability of all personal data in the systems and organization of the Group entities is maintained at all times. Therefore, not only those taking care of the infrastructure of the Group entities (IT, building), but all employees are personally responsible for ensuring data security and shall keep confidential any personal data to which the employees have gained access at work or in the context of their employment relationship with the Group entity. As a general rule, it is not allowed to take printed copies of work-related documents or data carriers off-premises. All employees shall only electronically communicate work-related matters via secure networks using secure systems, where possible. All employees are required to consult the Group's IT Acceptable Use Policy for more detailed information on how to use the Group's IT resources.

10. We will make sure these rules are followed from the beginning.

All employees are required to ensure that whenever they design a system, plan a project or otherwise set up or modify an activity that involves the processing of personal data, these rules are complied with from the beginning and that the Group entity can honour requests of data subjects exercising their rights as per Section IV.A ("privacy by design"). Also, when data subjects can choose how the Group entity processes their personal data, the Data Activity Owner shall, by default, opt for the most privacy-friendly processing option ("privacy by default"). This is especially important when providing online services and using apps for registered users.

11. We will train and raise awareness among employees for data protection.

The Group entities will make sure that all employees are aware of their tasks in connection with ensuring data protection compliance and that they receive regular data protection training in relation to their role and area of responsibility, as part of our trainings for new

hires and for existing employees. Such Training shall support employees, in particular Data Activity Owners, to understand their obligations under this Policy and under applicable Data Protection Law. Training completion records will be kept by Human Resources locally. All employees will be required to commit themselves to confidentiality.

12. We will cooperate with supervisory authorities.

All employees are required to ensure that requests by data protection authorities ("**Supervisory Authorities**") are forwarded to the DPC immediately to ensure appropriate handling of such requests. The DPC is responsible for the appropriate handling of such requests, including appropriate consultation with internal stakeholders, such as legal and compliance, liaising with external legal advisors, and providing timely responses to the Supervisory Authorities.

B. Further Rules for Special Situations

1. Using Third Parties

If a Group entity uses third parties, such as service providers, individual contractors or other Group entities, certain restrictions under Data Protection Laws apply if these other parties are given access to personal data or are asked to process it. Depending on the role of the third party, the Data Activity Owner shall ensure, together with the DPC, that a sufficient legal ground for their access to personal data exists.

If a Data Activity Owner wishes to engage such a third party at a Group entity, the Data Activity Owner shall, in consultation with the DPC:

(i) clarify the third party's role from a data protection law point of view, in particular whether it is a "processor" (i.e. somebody processing entirely under our instruction with us keeping control), a "controller" (i.e. somebody being itself responsible for the processing), a "joint controller" (i.e. somebody with whom we jointly decide over the processing) or an individual acting under our instruction (such as a consultant pursuant to Article 29 GDPR);

(ii) assess whether the third party is skilled and trustworthy and whether it provides for adequate data security to be entrusted with the personal data at issue;

(iii) have the necessary contractual clauses put in place, including a data processing agreement in the case of a "processor", a "joint controller agreement" in the case of a "joint controller" or, at a minimum, a non-disclosure agreement in the case of a "controller" or an individual acting under our instruction (such as a consultant pursuant to Article 29 GDPR),

(iv) give appropriate instructions to the third party, where applicable, and

(v) consult the DPC of the Group entity or legal counsel on all steps and assess whether it is permitted for the Group entity to even allow the third party to have access to the personal data, even if only as a service provider.

The process shall be documented by the Data Activity Owner, with the support of the DPC.

2. Exporting Personal Data

Whenever a Group entity makes personal data available to a recipient in a country other than Switzerland, the United Kingdom, or the EEA (among others), certain restrictions apply under Data Protection Laws. This includes granting remote access to somebody abroad (but it does not include online publications).

If a Group entity wishes to make personal data available to a recipient in another country (except to other Group entities who have signed the IGDTA, see Section IV.F), the Data Activity Owner shall (i) determine, with the support of the DPC, whether the recipient is in a country with an adequate level of data protection, (ii) if not, provide all necessary information to the DPC to allow the DPC to make an assessment of the risk of potentially unlawful access by foreign authorities upon making the data available to the recipient abroad as required by applicable Data Protection Law, and depending on the outcome, (iii) take steps to conclude a suitable data transfer agreement between the Group entity and the recipient and impose all other necessary supplementary measures upon the recipient to protect the personal data while in the hands of the recipient; or, if this is not possible or if the risks determined by the DPC in its assessment in (ii) remain too high (iv) determine another solution for the intended project together with the DPC to comply with international data transfer requirements. The DPC of the Group entity shall liaise with legal counsel as deemed necessary to comply with the international data transfer requirements.

The process shall be documented by the Data Activity Owner, with the support of the DPC.

3. Automated Individual Decisions, Profiling

Whenever a Group entity lets a computer make a discretionary decision over an individual or evaluate personal characteristics of an individual ("profiling"), which can have a legal or similarly significant effect on the individual (e.g., refusal or performance of a contract), certain restrictions under Data Protection Laws apply.

If automated decisions are necessary, the Data Activity Owner shall ensure that (i) the preconditions under applicable Data Protection Laws (e.g., the automated individual decision is necessary to conclude or perform a contract) are satisfied;(ii) the data subject has the right to be heard by a human and to require that the decision be re-evaluated by them; (iii) the Group entity's privacy notice refers to these decisions, and (iv) the Data Activity Owner consults with the DPC at the Group entity, the Group DPO or legal counsel before implementing an automated decision-making system to verify compliance with Data Protection Laws.

The process shall be documented by the Data Activity Owner, with the support of the DPC.

C. Responsibility for Compliance

Ensuring compliance with the above rules and those in Section IV at each Group entity is the responsibility of each employee. Business owner(s) of those business activities where processing of personal data occurs or for which such processing is undertaken; and of any person with management or other partial or full control over such processing shall monitor compliance within their responsibility. Further details, including a description of the roles and responsibilities, are contained in Exhibit A (Governance).

D. Exceptions

Under certain conditions, applicable law permits the Group entity to deviate from these basic principles and further rules for processing personal data. However, any such deviation shall be reviewed by the DPC to ensure that it complies with the law and approved by the business manager with the relevant compliance risk ownership in general or in a particular instance, following consultation with the DPC of the Group entity at issue, the Group DPO or legal counsel. The process shall be documented by the Data Activity Owner, with the support of the DPC.

IV. GOVERNANCE

A. Data Subject Requests

Data subjects have a number of rights that they can assert whenever the Group entities are controlling the processing of their personal data. Unless applicable Data Protection Law provides otherwise (e.g., to protect third parties or business secrets in case of access requests), the Group entity will take steps to comply with corresponding requests of data subjects. Group entities are subject to time limits for doing so. Before responding to a request, the DPC must make sure that the requestor has been properly identified.

These rights of data subjects include:

(i) the right to access and get a copy of the personal data the Group entity processes about them plus certain ancillary information;

(ii) the right to rectify inaccurate or incomplete personal data;

(iii) the right to ask the Group entity to restrict or otherwise object to the processing of their personal data;

(iv) the right to ask the Group entity to delete their data ("right to be forgotten");

(v) the right to ask the Group entity to tell the third parties with whom the Group entity has shared personal data about a particular data subject request;

(vi) the right to get a copy of the personal data the Group entity got from a data subject to allow the data subject to use it with another controller ("right of data portability");

(vii) the right to withdraw consent at any time; and

(viii) the right to object, on grounds relating to the data subject's particular situation, at any time to processing of their personal data, in particular, if the processing is based on an overriding "legitimate interest".

These rights can usually be exercised free of charge and without giving reasons.

If you, as an employee, receive such a request, you shall immediately forward it to the DPC. If you are unsure how to handle a specific request, consult the DPC of your Group entity, the Group DPO or legal counsel in such cases to verify compliance with applicable Data Protection Laws. The process shall be documented by the DPC.

At each Group entity, the management may designate a person or create a role for handling data subject requests. If such a person has been designated, the DPC shall forward the request to the person for further handling. Absent such a person or role, the DPC of the Group entity shall handle these requests themselves. The responsibility for decisions to object to a request shall, however, be taken by the management of the Group entity upon consultation of the DPC and, in cases that are likely to result in litigation, the Group DPO or legal counsel.

B. Data Breaches

If there is a breach in data security, i.e. when the confidentiality, integrity, availability or resilience of the personal data we process is breached intentionally or accidentally, resulting, for instance, in an unauthorized or unlawful disclosure, loss or alteration of personal data (e.g., information sent to the wrong recipient, loss or theft of an unprotected data carrier, cyber-attacks, etc.), the Group entity is required by Data Protection Laws to (i) immediately take measures to stop the breach and mitigate the potential negative impact on data subjects; (ii) to investigate the data breach (including root cause analysis), (iii) to assess the severity and probability of potential negative impact for the data subjects concerned, (iv) to notify the competent Supervisory Authorities of breaches that bear relevant risks for data subjects and to do so as soon as possible, but in any event within 72 hours upon our knowledge, (v) in special cases also to inform the data subjects, (vi) to take measures that will prevent such data breaches in the future, and (vii) keep a record of each data breach, its assessment and the steps taken.

If the Group entity processes personal data as a processor for somebody else (acting as a controller), the Group entity must in any event immediately notify this other person.

If you, as an employee, become aware of any actual or suspected data breach, whether due to your own fault or not, you are obliged to immediately inform the **Data Breach Contact Point** within your organization and, in the absence of such a person, the DPC. The person(s) will set the Data Breach Response Group in motion and instruct you on the further steps to take, if any.

The **Data Breach Response Group** shall immediately convene and ensure compliance with the obligations as indicated above and laid out in the applicable Data Protection Laws; the Group DPO, if applicable, shall be kept informed at all times and consulted prior to any notification. The management of each Group entity is responsible to (i) implement a suitable Data Breach Contact Point, (ii) have in place a Data Breach Response Group consisting of representatives of IT, information security, legal, the DPC and senior management (with the DPC maintaining the records) and with a head and deputy, (iii) provide for the necessary procedures and instructions and (iv) keep the Group DPO informed.

Any notification to an authority or third parties shall be made exclusively by the Group DPO unless Data Protection Laws require a legal representative of the Group entity to notify or the Group DPO delegates such task to the DPC, the head of the Data Breach Response Group or any other person at the relevant Group entity. The DPC of the Group entity shall keep the required records and provide the Group DPO with a copy.

C. Records of Processing Activities

The Group entity is required to keep an inventory of its activities for which the Group entity processes personal data as part of its business (e.g., payroll, personnel file, recruitment, direct marketing), whether in its capacity as a controller or processor. This must be done for each Group entity. Data Protection Laws set forth what information must be included in this record of processing activities, and the DPC and Group DPO may require that additional relevant information is included in the records of processing activities.

The records shall be maintained by the DPC of the Group entity (who shall be responsible, with the help of legal counsel, as necessary, for making sure that they contain the necessary information), but it is the responsibility of the business owner of each processing activity to notify the DPC about all processing activities and to provide all necessary information to the DPC to allow the DPC to prepare and maintain the records of processing for all processing activities. Employees are required to provide all necessary information to the DPC, either upon request or whenever a processing activity changes, to enable the DPC to keep the records of processing activities up to date. Each record of processing activities shall identify the Data Activity Owner who is responsible for the processing activity. A copy of the records is to be provided to the Group DPO whenever they are created or updated.

D. New Processing Activities

Whenever a new activity involving the processing of personal data is undertaken, or an existing processing

of personal data is planned to be modified in a material manner, the Group entity must ensure that it complies or continues to comply with this Policy and the applicable Data Protection Laws.

In order to do so, the Data Activity Owner must, in particular, verify and document that (i) the basic principles (in Section III) are complied with (subject to any exceptions pursuant to Section III.D); (ii) the further rules (in Section III.B) are complied with (subject to any exceptions pursuant to Section III.D); (iii) the records of processing activities are updated according to Section IV.C, and (iv) where necessary, a data protection impact assessment (DPIA) and/or a legitimate interest assessment has been carried out in consultation with the DPC.

A DPIA shall document the processing activity, the potential negative effects on the data subjects, the measures to prevent or mitigate those effects and the overall level of risk for the data subjects despite the measures implemented. If the residual risk remains high, the competent Supervisory Authorities may have to be consulted in accordance with applicable Data Protection Laws. A DPIA is necessary for processing activities that are likely to present a high risk for the data subjects, which is further defined in the applicable Data Protection Laws.

It is the responsibility of the Data Activity Owner to (i) ensure compliance with this Policy and the applicable Data Protection Laws, and (ii) initiate the process of verifying and documenting it with the assistance of the DPC of the relevant Group entity or legal counsel. This includes performing a DPIA in accordance with Data Protection Laws. The DPC shall keep a record of the documentation and provide the Group DPO, if applicable, with a copy.

The management of the Group entity shall establish the necessary procedures to ensure compliance with the foregoing.

E. Awareness, Training and Further Information

Each employee is required to (i) study this Policy, determine how it applies to their function and comply with it, (ii) undertake initial and refresher data protection training as offered by the Group or Group entity and as appropriate in view of their function, (iii) study the information provided by the Group and Group entity to data subjects with regard to the processing of their personal data (privacy notices, etc.) and act in accordance with such information (i.e. if we tell data subjects that we process their data only in a particular manner, we generally have to comply with this statement, and if we cannot, we have to change what we tell data subjects), (iv) consult further guidance offered by the Group and Group entity on how to comply with this Policy and applicable Data Protection Laws, and (v) consult the DPC of the Group entity or legal counsel, if issues remain unclear or the employee is not sure on how to handle the processing of personal data or comply.

F. Intra-Group Data Transfer Agreement

The transfers of personal data and "controller-processor" delegations of personal data processing within the Group shall be governed by an Intra-Group Data Transfer Agreement (**IGDTA**) to which each Group entity shall be a party. The entity of the Group DPO shall be the IGDTA's steward and have it updated as necessary. Each Group entity shall provide the Group DPO with any information and support requested for implementing the IGDTA and keeping it updated and in line with applicable Data Protection Laws.

G. Data Protection Roles

The responsibility for compliance with applicable Data Protection Law rests with each Group entity and its management with regard to the processing activities controlled by it. Each employee is required to take all reasonable steps as set out in this Policy to support the Group entity in its compliance with applicable Data Protection Law and to omit any activities that violate applicable Data Protection Law and this Policy.

The management of each Group entity shall provide the Group DPO with a report on the entity's data protection compliance at least on a yearly basis. The entity's compliance may be audited upon the Group DPO's, Group management's request or upon the Group internal audit's initiative, and the Group entity shall fully support such audits.

The **Group DPO** shall be responsible for managing the Group's data protection compliance, including setting the minimum standards of data protection applicable within the Group and the activities of the DPCs. The Group DPO shall be given the independence and resources necessary for fulfilling its task in a reasonable manner. The DPCs shall have a dotted reporting line to the Group DPO. The Group DPO shall have the right to verify each Group entity's data protection compliance,

to receive any requested information and access and to give corresponding instructions. The Group DPO shall be consulted on any material issue related to data protection and shall have a solid reporting line to the Group's senior management. The Group DPO shall provide the Group's senior management with a report on the Group's data protection compliance at least on a yearly basis and may directly bring any issue concerning the compliance with this Policy and Data Protection Laws to the attention of such senior management. If the responsibilities pursuant to this Policy are unclear or in dispute in a particular matter, the Group DPO shall rule on them, with escalation to the management of the Group entity (if the responsibilities are limited to such entity) or the Group's senior management.

The management of each Group entity shall appoint a **Data Protection Coordinator**, and/or if required by applicable Data Protection Law, a **Data Protection Officer** (collectively referred to as **DPC**) for managing data protection compliance at such entity and assisting the entity in its data protection compliance obligations, at the entities cost and responsibility. The management of each Group entity is required to comply with any requirements when appointing a Data Protection Officer, including notifying the appointment to the competent Supervisory Authority. Several entities may appoint the same DPC, but the DPC shall be employed by one of the Group entities. The DPC shall be given the independence and resources necessary for reasonably fulfilling its task. Exhibit A (Governance) sets forth further details.

V. OTHER

A. Sanctions

Violation of applicable Data Protection Law can result in serious sanctions by Supervisory Authorities and, under certain national laws, in personal criminal liability. Under the GDPR, administrative sanctions for intentional or unintentional violations of the GDPR can amount up to 4% of the total worldwide annual turnover or EUR 20 million, whichever amount is higher. Under the revised Swiss DPA, personal fines of up to CHF 250'000 are possible for violations with intent or willful blindness. Further, the Group's entities may be ordered to stop or change certain processing activities and may be subject to civil claims by data subjects.

Accordingly, it is important that all employees comply with this Policy, whether as a regular employee or in a special role provided for in the Policy. Failure to comply with this Policy can result in sanctions under the employment agreement, including termination.

B. Revisions

The owner of this Policy is the Group DPO. It shall be revised as necessary and reviewed at least annually. The Group DPO has the right to issue further policies detailing the obligations and other provisions contained in this Policy, subject to formal approval by the Group's senior management.

Approved and issued by Marina Souza, Fyffes Head of Legal, in January 2024.

Exhibit A

GOVERNANCE

This Exhibit further details the functions relevant for compliance with data protection law and is based on the Group Data Privacy Policy (the **Policy**), in particular Section III.C and Section IV.G.

The following applies to **each Group entity**:

- The **Board of Directors** has the ultimate responsibility for the Group entity's compliance with applicable data protection law and, in the Group context, with the Policy. It shall:
  - Have a basic understanding of applicable Data Protection Law and the requirements of the Policy;
  - Require Management to implement the Policy to ensure the entity's compliance with applicable Data Protection Law and the Policy at an operational level;
  - Study compliance reports provided, investigate indications of non-compliance and take necessary remedial actions in consultation with the Group DPO and Group Management;
  - Provide reports as to the entity's compliance with applicable Data Protection Law and the Policy to the Group Management and the Group DPO (i) on a regular basis (at least yearly), (ii) in case of material developments, and (iii) if requested.

- The **Management**, in particular the **CEO**, has the operational responsibility of the Group entity's compliance with applicable data protection law and the Policy. It shall:
  - Have a basic understanding of applicable Data Protection Law and the requirements of the Policy;
  - Issue the instructions necessary to have the Policy implemented and complied with at the entity, including (i) by appointing the necessary functions (including as provided for in this Exhibit), and (ii) by establishing the processes necessary for compliance with the Policy;
  - Ensure that applicable Data Protection Law is complied with at the entity in addition to the provisions of the Policy;
  - Ensure that where tasks are delegated, the delegates are properly selected, instructed and supervised by Management;
  - Study compliance reports provided, investigate indications of non-compliance and take necessary remedial actions in consultation with the DPC and the Group DPO;
  - Provide reports as to the entity's compliance with applicable Data Protection Law and the Policy to the Board of Directors and the Group DPO (i) on a regular basis (at least yearly), (ii) in case of material developments, and (iii) if requested.
- Each activity of processing personal data (the **Activity**) shall have at least one **Data Activity Owner** (**DAO**), who shall be responsible (alone or with other DAOs of the same Activity) for the compliance of such Activity with applicable Data Protection Law and the Policy.

  Unless decided otherwise by Management in a specific case, the DAO of an Activity is its "beneficiary" in the first line of defence, i.e. the business owner(s) of those business activities where the processing of personal data occurs and for which the Activity is undertaken.

  Furthermore, any other person with management or other partial or full control over such processing shall be considered a DAO; "control" shall mean the legal or de-facto power to take, or actual taking, of decisions concerning aspects of the Activity that are essential for its compliance with the Policy or applicable Data Protection Law (e.g., which categories of personal data are collected, the categories of recipients of personal data, the retention periods).

  If there are several DAO for the same activity, each DAO is responsible for their own decisions and those of any DAO who is subordinate to such DAO. It shall:
  - Have an understanding of applicable Data Protection Law and the requirements of the Policy with regard to the Activity;
  - Select the appropriate staff and issue the instructions necessary to have the Policy and the additional requirements of applicable Data Protection Law implemented and

complied with at the entity with regard to the Activity, and supervise the proper execution of the instruction, including by requesting appropriate reports;
- Take decisions with regard to the Activity only in compliance with the Policy and the additional requirements of applicable Data Protection Law and upon consultation of the DPC and, where appropriate, with the Group DPO; where the DAO concludes that it cannot or does not want to take a decision, it shall escalate it to its superior, who shall then become a DAO, as well.
- Study compliance reports provided with regard to the Activity, investigate indications of non-compliance and take necessary remedial actions in consultation with the DPC and, where appropriate, the Group DPO;
- Provide reports as to the Activity's compliance with applicable Data Protection Law and the Policy to the Management (i) on a regular basis (at least yearly), (ii) in case of material developments, and (iii) if requested;
- Notify themselves to the DPC, who shall keep track of them.

- The **DPC** shall be responsible for managing the data protection compliance activities at the entity and assisting the other functions in their data protection compliance obligations. It shall:
  - Have a detailed understanding of applicable Data Protection Law and the requirements of the Policy;
  - Be independent, i.e. not hold any interest in the personal data processing activities of the entity;
  - Unless provided otherwise manage the data protection processes and other data protection compliance activities of the entity and undertake the DPC tasks provided for in the Policy in compliance with the Policy;
  - Advise and support the DAOs and the Management with regard to their responsibility for complying with applicable Data Protection Law and the Policy;
  - Monitor the DAOs compliance with applicable Data Protection Law and the Policy;
  - Consult the Group DPO on any material issues concerning the entity's compliance with applicable Data Protection Law or the Policy, or when unsure;
  - Provide reports as to the entity's compliance with Data Protection Law and the Policy to the Management, to the Board of Directors and to the Group DPO (i) on a regular basis (at least yearly), (ii) in case of material developments, and (iii) if requested;
  - Not have or assume any decision-making power (including right to veto or interfere) with regard to any specific processing or other data protection compliance activity of the entity; in case of a suspected or actual non-compliance, this shall be reported to the Management (and Group DPO), who shall take the necessary decision or remedial action (with the Group DPO requesting such decision or action from Group Management);
  - In case the DPC has also been formally appointed as Data Protection Officer pursuant to Art. 38 GDPR fulfill all tasks of a DPO pursuant to Art. 39 GDPR to the extent these tasks are not already covered by the above.

The following applies to the **Group level**:

- The **Group Board of Directors** and its members (not acting in their capacity as officials of a particular Group entity) sets forth the overall framework for ensuring compliance with applicable data protection (including by issuing this Policy). They:
  - Shall have a basic understanding of applicable Data Protection Law;
  - Have the right to issue binding Group-wide policies concerning the processing of personal data and compliance with applicable Data Protection Law;
  - Hereby requires Group Management to implement the Policy at the Group level to ensure the Group's compliance with applicable Data Protection Law and the Policy;
  - Will study compliance reports provided, investigate indications of non-compliance and take necessary remedial actions in consultation with the Group DPO and Group Management;
  - Will, except as laid out in the foregoing, not assume any decision-making power with regard to any specific processing of personal data or other specific data protection compliance activity of a particular Group entity (unless acting in its capacity as the Board of Directors of such entity).

- The **Group Management**, in particular the **Group CEO**, has the operational responsibility of the Group's compliance with applicable Data Protection Law and the Policy. It shall:
  - Have a basic understanding of applicable Data Protection Law and the requirements of the Policy;
  - Issue the instructions necessary to have the Policy implemented and complied with at the Group, including (i) by appointing the necessary Group functions (including as provided for in this Exhibit), and (ii) by establishing the Group processes necessary for compliance with the Policy;
  - Ensure that applicable Data Protection Law is complied with by the Group in addition to the provisions of the Policy;
  - Ensure that where tasks are delegated at Group level, the delegates are properly selected, instructed and supervised by Group Management;
  - Study compliance reports provided, investigate indications of non-compliance and take necessary remedial actions in consultation with the Group DPO;
  - Provide reports as to the Group's compliance with applicable data protection law and the Policy to the Group Board of Directors (i) on a regular basis (at least yearly), (ii) in case of material developments, and (iii) if requested.
- The **Group Data Protection Officer** (**Group DPO**) shall be responsible for managing the data protection compliance activities at the Group and assisting the other functions in their data protection compliance obligations. It shall:
  - Have a detailed understanding of applicable Data Protection Law and the requirements of the Policy;
  - Be independent, i.e. not hold any interest in the personal data processing activities of the Group;
  - Manage the data protection processes and other data protection compliance activities of the Group and undertake the Group DPO tasks provided for in the Policy in compliance with the Policy;
  - Advise and support the DPCs, the DAOs, the Management of the Group entities and the Group Management with regard to their responsibility for complying with applicable Data Protection Law and the Policy;
  - Monitor the DAOs compliance with applicable Data Protection Law and the Policy in cases that are material for the Group;
  - Provide reports as to the Group's compliance with applicable Data Protection Law and the Policy to the Group Management and to the Group Board of Directors (i) on a regular basis (at least yearly), (ii) in case of material developments, and (iii) if requested;
  - Not have or assume any decision-making power (including right to veto or interfere) with regard to any specific processing or other data protection compliance activity of a Group entity; in case of a suspected or actual non-compliance, this shall be reported to the Group Management or Management of the entity, who shall take the necessary decision or remedial action.

In addition to the foregoing, **internal audit** functions shall independently verify the Group's compliance with applicable Data Protection Laws and the Policy and provide corresponding reports to the relevant management and board functions within the Group. All functions shall cooperate with internal audit.