**DATED** **2018**

# PANAYA EMPLOYEE PRIVACY POLICY

**CONTENTS**

## 1. PURPOSE

1.1 The purpose of this Policy is to outline the rules under which personal data of employees, is gathered, processed, used and stored, in order to ensure that this data is kept private and secure and in accordance with the applicable law regarding data protection and data secrecy to ensure regulatory compliance and for the protection of the Panaya group employees.

1.2 Through this Policy, Panaya wishes to illustrate its goal to comply with data protection laws in the countries in which it operates, to retain the trust of its Employees and to process Employee Data with confidence that consistent security mechanisms are in place wherever Panaya operates in the world.

1.3 This Policy is binding in its present form for Panaya Panaya Inc. and all subsidiaries controlled by it directly or indirectly (all or each individually hereto referred to as "Panaya") to the extent that the local data privacy laws in each country where each Panaya entity and relevant data subject reside, require Panaya to perform the actions contained herein.

## 2. DEFINITIONS

**"Archive"** means a collection of Employee Data that are no longer necessary to achieve the Purposes for which the Employee Data originally were collected or that are no longer used for general business activities, but are used only for historical or statistical purposes, dispute resolution, investigations or general archiving purposes.

**"Dependent Data"** means any information relating to an identified or identifiable individual where the individual is a dependent or family member of an Employee and whose personal data have been given to Panaya by an Employee or by such individual;

**"Employee"** shall mean an employee, job applicant, contractor or former employee or former contractor of Panaya;

**"Employee Data"** means any information relating to an identified or identifiable individual where the individual is an Employee as well as any Dependent Data;

**"GDPR"** means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (repealing the Data Protection Directive);

"**Israeli Law**" means the Protection of Privacy Law 1981 (the "Privacy Law"), the Protection of Privacy Regulations (data security) 2017 and any other applicable regulations or directives issued under the Privacy Law.

**"Information Security Incident"** means any actual or suspected theft, or unauthorized Processing, loss, use, disclosure, or acquisition of, or access to, any data;

**"Original Purpose"** means the Purpose for which Employee Data was originally collected;

"**Privacy Officer**" means the Panaya Data Protection Officer

**"Processing" ("Process", "Processed")** means any operation that is performed on Employee Data, whether or not by automatic means, such as collection, recording, storage, organization, alteration, use (including in a different context), disclosure (including the granting of remote

access), blocking, transmission or deletion of Employee Data. This includes for instance the use of electronic data on central systems or PC workstations but also access to e.g. data held in card indexes or paper files;

**"Processing Staff"** means all Employees and other persons who Process Employee Data as part of their respective duties or responsibilities using Panaya information technology systems or working primarily from Panaya premises;

**"Purpose"** means the purposes for Processing set out in schedule ;

**"Sensitive Data"** means Employee Data that reveal an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, criminal convictions and offences or related security measures, and any other data to the Processing of which particular conditions apply under applicable laws; and

**"Third Party"** means any person or entity (e.g., an organizations or government authority) outside Panaya.

## 3. KEY PRINCIPLES FOR THE PROCESSING OF EMPLOYEE DATA

3.1 Panaya respects and upholds its employees' right and need for privacy and strives to balance it with Panaya's need to protect its sensitive assets (including but not limited to: intellectual property, customer data, etc.) by gathering, and monitoring essential information. Therefore, Panaya will observe the following principles when Processing Employee Data:

3.1.1 Data will be Processed fairly and lawfully.

3.1.2 Data will be collected for specified, legitimate purposes and not Processed further in ways incompatible with those purposes.

3.1.3 Data will be relevant to and not excessive for the purposes for which they are collected and used.

3.1.4 Data will be accurate and where necessary, kept up-to-date. Reasonable steps will be taken to rectify or delete Employee Data that is inaccurate or incomplete.

3.1.5 Data will be kept only as long as it is necessary for the purposes for which it was collected and Processed.

3.2 Data will be Processed in accordance with the individual's legal rights.

## 4. POLICY

### 4.1 Objective: compliance with applicable rules and laws

This Policy is designed to provide a uniform compliant standard for Panaya worldwide with respect to the protection of its Employee Data. Panaya will handle Employee Data in accordance with the standards of the GDPR the Israeli Law, and US law as applicable, with appropriate outliers in countries where laws require lesser standards than those described in this policy herein.

**4.2 Processing: categories, purposes and basis**

4.2.1 Panaya Processes certain types of its Employee Data mainly for the purposes of the administration and management of its staff and its business and for compliance with applicable laws. Details on the kinds of Data and Processing purposes are included in **Schedule** .

4.2.2 Panaya may also Process different categories of Employee Data, and Process them for different Purposes, depending on the Employee's function. The full list of categories of Employee Data and Purposes listed in **Schedule** may therefore not be applicable to all Employees.

4.2.3 In any event, Panaya shall restrict the Processing of Employee Data for a particular Purpose to those Employee Data that are reasonably adequate for and relevant to the applicable Purpose.

4.2.4 This Processing may be:

4.2.4.1 necessary for the performance of its contracts with Employees,

4.2.4.2 necessary for compliance by Panaya with its legal obligations in relation to employment and social security,

4.2.4.3 necessary for the purposes of the legitimate interests pursued by Panaya, in particular its economic, commercial and financial interests, business continuity, security and confidentiality of customer information and products, security of digital and physical infrastructure, and

4.2.4.4 in certain circumstances, necessary in order to protect the vital interests of the Employee.

4.2.5 The Processing of Employee Data shall not generally be based on consent. However, if applicable local law so requires, in addition to the legal basis listed above, Panaya shall also seek Employee consent for the Processing. If none of the legal grounds above apply, Panaya may request Employee consent for Processing Employee Data, but only under certain circumstances.

**4.3 Secondary purposes of Processing**

Generally, Employee Data shall be used only for the Original Purposes. Employee Data may be Processed for a legitimate Purpose listed in schedule other than the Original Purpose (**"Secondary Purpose"**) only if the Original Purpose and Secondary Purpose are closely related.

**4.4 Special categories of Employee Data**

4.4.1 Sensitive Data: grounds for Processing

Panaya does not intend to collect and Process Sensitive Data but only does so to the extent necessary to serve the applicable Purpose and to the extent that the legal grounds for Processing permit the Processing of Sensitive Data. Panaya mainly collects Sensitive Data where an Employee is sending medical certificate to justify

an absence due to illness, or in order to comply with local legal requirements or specific in-country practices.

4.4.2 Dependent Data: the Employee who provides such Dependent Data to Panaya shall ensure that, prior to or at the latest at the moment of the providing of such Dependent Data to Panaya, the individual to whom the Dependent Data relates is duly informed of the contents of this Policy.

**4.5 Data retention: period and consequences**

4.5.1 Panaya generally shall retain Employee Data only:

4.5.1.1 for the period required to serve the applicable Purpose;

4.5.1.2 to the extent reasonably necessary to comply with an applicable legal requirement; or

4.5.1.3 as advisable in light of an applicable statute of limitations or of applicable legal hold and litigation document preservation requirements.

4.5.2 Panaya may specify a time period for which certain categories of Employee Data will be kept.

**4.6 Rights of Employees**

Personal data will be processed in accordance with the rights of the subject of the data under the applicable legislation, including (where applicable) right of access to own Employee Data, accuracy and right of rectification, and right to object or to withdraw consent.

**4.7 Security Requirements**

4.7.1 Data security

Panaya takes appropriate commercially reasonable technical, physical and organizational measures to protect Employee Data from misuse or accidental, unlawful or unauthorized destruction, loss, alteration, disclosure, acquisition or access. Furthermore, where Panaya uses any Third Party for Processing purposes, Panaya undertakes to comply with applicable obligations in relation to the elements to take into consideration when selecting such Third Parties and shall among other things require and check that respective technical, physical and organizational measures for protecting Employee Data are in place.

4.7.2 Processing Staff access

4.7.2.1 Processing Staff shall be provided access to Employee Data only to the extent necessary to serve the applicable Purpose as necessary to perform their tasks.

4.7.2.2 In addition, access is given to senior executives for global workforce management; to managers for managing their Employees; and to Employees for self-service maintenance of relevant data elements (such as address).

### 4.8 Transfer of Employee Data

4.8.1 Transfer of Employee Data includes situations in which one Panaya entity:

4.8.1.1 discloses Employee Data to another Panaya entity (e.g. other Panaya entities make Employee Data available to Panaya for global compensation),

4.8.1.2 discloses Employee Data to a Third Party (e.g. in the context of a contractual relationship with a provider of Employee benefits), or

4.8.1.3 provides remote access to Employee Data to another Panaya entity or to a Third Party (e.g. in the context of providing IT services to systems on which Employee Data are stored).

Any of the above may involve transfer of an Employee Data to a country outside the Employee's country of residence.

4.8.2 Transfer of Employee Data between Panaya entities or from Panaya to Third Parties as a general rule require the conclusion of a data transfer agreement between the involved parties, and Panaya shall ensure that an adequate level of protection of Employee Data is in place where required in the context of such transfer and Processing by Third Parties.

### 4.9 Compliance and Supervision

Panaya has appointed a DPO/Global Compliance Officer who will oversee compliance with this Policy and with Panaya 's data protection compliance activities. **Enforcement Rights and Mechanisms**

4.9.1 Panaya will ensure that this Policy is observed.

4.9.2 If at any time, a person believes that Employee Data relating to him or her has been processed in violation of this Policy, he or she may and should report the concern to the appropriate DPO/Privacy Officer or to his or her manager.

### 4.10 Training

Panaya shall provide training on this Policy and other privacy and data security obligations to Processing Staff and to Employees tasked with the monitoring and enforcement of this Policy (e.g. Privacy Officers, HR managers).

### 4.11 Sanctions

Non-compliance of Panaya Employees with this Policy may result in disciplinary action up to and including termination of employment.

### 4.12 Changes to this Policy

Panaya reserves the right to modify this Policy as needed, for example, to comply with changes in laws, regulations, Panaya practices and procedures, or requirements imposed by data protection authorities. Panaya 's DPO/Global Compliance Officer, or his or her designee, must approve all changes to this Policy for them to become effective. Panaya will inform its Employees of any material changes in the Policy.

## 5. QUERIES

Any queries relating to this Policy should be directed to the DPO/local Privacy Officer (as defined hereunder), who will be able to provide guidance as to its application and to provide guidance regarding conflicts with other Panaya group policies where they may arise.

DETAILED CONSENT FORM FOR PANAYA DATA PRIVACY PRACTICES
(To be signed electronically, unless requested otherwise)

I have read the Panaya Data Privacy Policy and I consent to the collection, the processing and the transfer of my personal data as outlined in this policy. I understand that my data may be accessed from outside my country of work to allow Panaya to process my data in the course of my employment.

I understand that I have the right to access my data, and seek to have it altered if necessary, in accordance with the principles adopted by Panaya.

I confirm that I understand the contents of this document written in English, and I do not require any translation or explanation to the document

I acknowledge that my consent is rendered voluntarily after being informed of my right to withhold my consent and I am not required to provide any data under law. However, I understand that by applying for employment and or by being employed by a Panaya entity, collection, processing and transfer of my personal data in accordance with the above policy is required.

| Schedule 1: Categories of Employee Data processed, and purposes of processing | | | | | |
|---|---|---|---|---|---|
| **Processing of Employee Data** | **Purposes of processing** | | | | |
| **Categories of personal data** | **1** | **2** | **3** | **4** | **5** |
| **Personal identification data:** name, addresses, telephone numbers, passport number, etc. | V | | | | |
| **Electronic identification data:** IP addresses, connection logs, etc. | V | | | | V |
| **Financial data:** bank account numbers, insurance, revenue & income, etc. | V | | | | |
| **Personal characteristics:** age, sex, date of birth, place of birth, citizenship, visa details, etc. | V | V | V | | |
| **Physical characteristics:** height, weight, Clothes size, hair colour, distinctive marks, etc. | | V | | | |
| **Lifestyle:** social contacts (friends, etc.), travel details, consumation habits, etc. | | V | | | |
| **Family:** marital status, cohabitation, spouse/partner name, children, parents, etc. | V | V | | | |
| **Hobbies**: hobbies, interests, sport, etc. | | V | | | |
| **Judicial data:** data on suspected offences & crimes, on criminal sentences, on administrative penalties & fines, etc. | V | | | | |
| **Consumption habits:** car or other vehicle ownership (or leased status), vehicle type and registration, other goods & services provided or lent to or by the data subject. | V | | | | |
| **Housing:** Address, kind of housing, length of stay in housing, etc. | V | | | | |
| **Health-related data:** physical health, psychological health, risk-inducing behaviour & situations, genetic data, treatment data. | V | | | | |
| **Education:** studies curriculum, financial history of studies, qualifications, professional experience, publications, etc. | V | | | | |
| **Profession & employment:** current employment, function, task description, recruitment data, data on end of employment, career data, salary, work management & organisation, security (passwords & passcodes, security level), data on use of computer resources, etc. | V | | | | |
| **National identification number & social security number** | V | V | | | |
| **Image recordings:** photos, videos (e.g. CCTV) | V | V | | | |

**Reference ID in matrix below:** **Purpose:**

**1** Staff-related administration:

- salary & commission management
- recruiting and selection of personnel and interim employees
- application of employment law
- Welfare

**2** Staff management:

- assessment of personnel and follow-up
- career planning and training

**3** Work allocation:

- planning and allocation of tasks, workload and work

**4** Control in the workplace:

- physical control of performance in the workplace (e.g. using CCTV or behavioural monitoring)
- control of use of digital equipment and tools (e.g. logs and systems for the monitoring of e-mail or Internet use)

**5** Security:

- protection of the security of goods and personnel