Expereo Data Privacy Code

*The term “Expereo” refers to Expereo International B.V and its affiliates (https://www.expereo.com/contact)

Expereo contact:

Sujata Kukreja -Chief Compliance Officer
Email: sujata.kukreja@expereo.com

1. Introduction

Expereo is committed to ensure the protection of personal data in compliance with the General Data Protection Regulation (GDPR) and other applicable data protection laws. This Data Privacy Code for Data Processing (the "Data Privacy Code") is meant to provide the framework for Expereo's global data protection practices, particularly for the transfer of personal data from the European Economic Area (EEA) to non-EEA countries.

This Data Privacy Code is legally binding across all Expereo Affiliates and create enforceable rights for data subjects, ensuring that personal data is handled responsibly and transparently, regardless of geographic location.

2. Definitions

2. 1 **"Adequacy Decision"** an adequacy decision permits a cross-border data transfer outside the EU, or onward transfer from or to a party outside the EU without further authorization from a national supervisory authority.

2. 2 **"Binding Corporate Rules"** means a privacy policy framework considered to provide an adequate level of protection for the transfer of Personal Data within a group of companies under Applicable Law.

2. 3 **"Controller**" means an entity that determines the purposes and means of the processing of Personal Data.

2. 4 **"Data Subject"** means any identifiable natural person whose personal data is being collected, held or processed.

2. 5 **"Data Protection Laws**" means all data protection and privacy laws applicable to the processing of Personal Data by Expereo on behalf of the Data Subject for a legitimate business purpose.

2. 6 **"Expereo Group"** means all Expereo International B.V, its parent company, subsidiaries and affiliates, and any other entities controlled by or under common control with Expereo International B.V, whether directly or indirectly.

2. 7 **"EU SCCs"** means the Standard Contractual Clauses used for personal data transfers to a country outside the European Economic Area (EEA) without an Adequacy Decision.

2. 8 **"GDPR"** means the General Data Protection Regulation (EU) 2016/679 as amended or replaced from time to time.

2. 9 **"Personal Data"** as used in this Data Privacy Code means any information relating to an identified or identifiable natural person that Expereo processes on behalf of Data Subject for a legitimate business purpose

2. 10 **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

2. 11 **"Processor"** means an entity that processes Personal Data on behalf of a Controller.

2. 12 **"Sub-Processor"** means a Processor engaged by Expereo that processes Personal Data pursuant to the Agreement.

All rights reserved Copyright@ Expereo DPA 2024

3. Scope

This Data Privacy Code apply to:

a) All Expereo group entities that process personal data.

b) All processing of personal data, including but not limited to customer data, applicants and employee data and supplier data.

c) All transfers of personal data from the EEA to non-EEA countries within Expereo group.

3.1. Employee's data

As part of the employment relationship, Expereo processes personal data of its employees in accordance with applicable data protection laws, including the General Data Protection Regulation (GDPR).

3.1.1. Legal Basis for Processing

Employee personal data is processed as necessary for the performance of the employment contract, for compliance with legal obligations, and where relevant, based on Expereo's legitimate interests in ensuring the effective operation and security of its workplace.

By entering into the employment contract, employees acknowledge and agree that their personal data may be collected, processed, and stored by Expereo for employment-related purposes.

3.1.2. Location Data

Expereo may collect and process employee location data solely for the purpose of monitoring attendance and presence at the office premises. This data is used to support workplace operations, fulfill health and safety obligations (e.g., evacuation protocols), and ensure adherence to work schedules.

Access to location data is restricted to authorized personnel and is processed in a proportionate manner, consistent with the intended purpose.

3.1.3. CCTV Monitoring

Expereo may install closed-circuit television (CCTV) cameras in common public areas (e.g., entrances, hallways, lobbies) for the following purposes:

- Ensuring the safety and security of employees, visitors, and property;
- Preventing and investigating incidents of theft, vandalism, or misconduct;
- Complying with applicable safety and security regulations.

CCTV footage is not used for employee performance evaluation and is retained for a limited period in accordance with applicable retention policies, unless required for the investigation of an incident.

3.1.4. Data Access and Protection

All personal data collected is accessed only by authorized personnel and safeguarded through appropriate technical and organizational measures. Employees have the right to access, rectify, or restrict the processing of their data as permitted by law.

For more information on your data protection rights, or to raise concerns, please contact legal@expereo.com or your local HR representative.

All rights reserved Copyright@ Expereo DPA 2024

3.2. Applicants

Please refer to Expereo Recruitment Privacy Policy

3.3. Other data subjects

Please refer to Expereo Register of Data Processing Activities

4. Principles for processing

Expereo is committed to processing personal data in compliance with the following core principles derived from the GDPR:

- **Lawfulness, fairness, and transparency**: Personal Data will be processed in a lawful, fair, and transparent manner.
- **Purpose limitation**: Personal Data will be collected for specific, explicit, and legitimate purposes and not processed further in a way incompatible with those purposes.
- **Data minimization**: Personal Data will be adequate, relevant and limited to what is necessary for the legitimate business purpose.
- **Accuracy**: Personal Data will be accurate and kept up to date if necessary.
- **Limited retention period**: Personal Data will not be retained for longer than necessary.
- **Security and confidentiality**: Personal data will be processed in a manner that ensures appropriate security, including protection against unauthorized access or disclosure.

5. Rights of Data Subjects

The Expereo guarantees that the Data Subjects have enforceable rights, including:

- **Access**: Data Subjects have the right to access their Personal Data held by Expereo
- **Rectification**: Data Subjects have the right to correct inaccurate or incomplete Personal Data.
- **Deletion ("Right to be Forgotten"):** Data Subjects can request deletion of their Personal Data under certain circumstances.
- **Data Portability**: where technically feasible, Data Subjects may request the transfer of their Personal Data.
- **Right to object**: Data Subjects may object to the processing of their Personal Data, including for marketing purposes.

These rights are enforceable against all Expereo group, including where personal data is transferred outside the EEA.

5.1. Contact details

If you would like to contact us in regard to the processing of your personal data, or exercise any of the rights set out above, please send an e-mail to legal@expereo.com.

All rights reserved Copyright@ Expereo DPA 2024

6. Transfers of Personal Data

When transferring personal data to third-party Data Processors, Expereo ensures that such transfers are subject to appropriate safeguards, such as:

- Contracts that impose obligations to protect personal data in line with the Group's standards and GDPR requirements.
- Ongoing monitoring of the third-party's compliance with data protection obligations A processing of Personal Data under the responsibility of Expereo may involve a transfer of Personal Data outside of the European Union (such as to the United States of America and the United Kingdom).

In such cases Expereo always remains the Controller. In the absence of Adequacy Decisions Expereo uses the EU SCCs for use between controller and controller (module one) and between controller and processor (module two) as grounds for legitimizing such a transfer.

All Expereo non-EEA entities will provide equivalent levels of protection for Personal Data as required under GDPR.

7. Responsibilities of Expereo Group entities

Each entity within Expereo Group is responsible for:

a) Implementing this Data Privacy Code at a local level, ensuring that data protection practices align with Expereo global standards.

b) Cooperating with internal and external audits of data protection compliance.

c) Reporting any data breaches to the central Data Protection Officer (DPO) within 72 hours of discovery and assisting in notifying the relevant supervisory authorities and data subjects when required.

8. Compliance and monitoring

To ensure compliance with this Data Privacy Code, Expereo will implement the following:

a) Training: All employees who process personal data will undergo data protection training tailored to their role.

b) Internal Audits: Regular audits will be conducted to assess compliance with these Data Privacy Code and other applicable data protection laws.

c) Data Protection Officer (DPO): Expereo Group has appointed a DPO responsible for overseeing data protection compliance, advising on data protection matters, and acting as a point of contact for supervisory authorities and data subjects

All rights reserved Copyright@ Expereo DPA 2024