Data Privacy Policy
CONTENTS

1 Introduction to Fingerprints Data Privacy Policy .................................................................3

2 Terms and Abbreviations .....................................................................................................4

3 Scope ....................................................................................................................................5

4 Legal ground for processing personal data ........................................................................5

4.1 Legal ground for processing biometric data ......................................................................5

5 Data quality requirements ..................................................................................................5

6 Communicating privacy information ..................................................................................5

7 The use of personal data ......................................................................................................6

7.1 The use of personal data within Fingerprints ....................................................................6

7.2 Biometric data .......................................................................................................................6

7.2.1 The collection of biometric data from employees ..........................................................6

7.3 Employee personal data ......................................................................................................7

7.4 Business contacts ..............................................................................................................7

8 Data subjects’ rights ............................................................................................................7

9 Big data analytics and profiling ..........................................................................................7

10 Compliance with GDPR ....................................................................................................7

11 Cyber security and data breaches .......................................................................................8

12 International transfers .......................................................................................................8

12.1 Outsourcing and cloud services .......................................................................................8

13 Consequences of failing to comply ..................................................................................8

14 Privacy organization ..........................................................................................................9

14.1 DPO responsibilities .......................................................................................................9

14.2 Information owner responsibilities ...............................................................................9

14.3 System owner responsibilities ......................................................................................10

14.4 Who is responsible for this policy? ..............................................................................10
1 INTRODUCTION TO FINGERPRINTS DATA PRIVACY POLICY

The Data Privacy Policy is a set of rules for protecting privacy data related to employees, contractors, partners & customers within the Fingerprint Cards Group.

Fingerprint Cards Group holds personal data about our employees, contractors, partners, customers and other individuals for a variety of business purposes.

This policy sets out how we within the company are to protect personal data. If you have any questions about it please contact the Data Protection Officer (DPO) at DPO@fingerprints.com.

Remember to consult the DPO before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.
2 TERMS AND ABBREVIATIONS

The table below describes the terms and abbreviations used in this document, if not explained elsewhere.

<table>
<thead>
<tr>
<th>Term/Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation (EU 2016/679) EU Legislation regarding the protection of privacy data</td>
</tr>
<tr>
<td>Privacy Shield</td>
<td>The EU-US Privacy Shield is a framework for transatlantic exchanges of personal data for commercial purposes between the European Union and the United States. <a href="https://www.privacyshield.gov/">https://www.privacyshield.gov/</a></td>
</tr>
<tr>
<td>Data Subject</td>
<td>An identified or identifiable natural person, see Personal Data</td>
</tr>
<tr>
<td>Business purposes</td>
<td>The purposes for which personal data may be used by Fingerprints: Personnel, administrative, financial, regulatory, payroll and business development purposes, including R&amp;D activities.</td>
</tr>
<tr>
<td>Personal Data</td>
<td>‘Personal data’ means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.</td>
</tr>
<tr>
<td>Sensitive Personal Data</td>
<td>‘Sensitive personal data’ means personal data revealing race/ethnic origin, political opinion, religion, union membership, health information, philosophical conviction, sexual life and genetic and biometric data.</td>
</tr>
<tr>
<td>Biometric Data</td>
<td>Personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or fingerprints.</td>
</tr>
<tr>
<td>DPO</td>
<td>Data Protection Officer, see <a href="#">Responsibilities of the DPO</a></td>
</tr>
<tr>
<td>Processing</td>
<td>‘Processing’ means any operation which is performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, reading, restriction, erasure or destruction.</td>
</tr>
<tr>
<td>Fingerprints</td>
<td>Fingerprint Cards Group</td>
</tr>
<tr>
<td>Privacy notice</td>
<td>A statement made to a data subject that describes how Fingerprints collects, uses, retains and discloses personal data</td>
</tr>
<tr>
<td>Controller</td>
<td>The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.</td>
</tr>
<tr>
<td>Processor</td>
<td>A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller</td>
</tr>
</tbody>
</table>
3 SCOPE

This policy applies to all employees, contractors, partners & suppliers who have access to or process personal data, all of whom must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to Internet and email use. We may supplement or amend this policy with additional policies and instructions from time to time, e.g. instruction on handling biometric data. Any new or modified policy will be circulated to staff before being implemented.

4 LEGAL GROUND FOR PROCESSING PERSONAL DATA

Fingerprints must always have a legal ground for any processing of personal data, and it will be if at least one of the following applies:

(i) Fingerprints has obtained consent from the individual,
(ii) Fingerprints has to process personal data to perform a contract with the individual,
(iii) Fingerprints has to process personal data to comply with a legal obligation, or
(iv) Fingerprints has a legitimate interest to process personal data and this interest outweighs the individual’s privacy interest (e.g. for certain direct marketing purposes, in the context of ensuring network and information security as well as for collecting business contact information).

4.1 Legal ground for processing biometric data

As biometric data is sensitive data, it can only be processed with the consent of the data subject. It is Fingerprints’ responsibility to prove that the data subject has consented to the processing of their biometric data. If Fingerprints uses biometric data collected with consent from a third party, the third party will have to be able to demonstrate that this is the case upon request from Fingerprints.

For consent to be valid, it has to be given freely, be specific, informed and unambiguous. It needs to be shown either by a statement or a clear affirmative action that signifies agreement to the processing.

5 DATA QUALITY REQUIREMENTS

Fingerprints must comply with applicable data quality requirements, i.e.:

(i) Personal data may only be collected for a specific purpose and not be further processed for other purposes which are incompatible with the initial purpose;
(ii) When personal data is collected, Fingerprints must inform the data subject about the retention period that the data is stored within the company. When this time is up the personal data must be deleted from Fingerprints’ systems.
(Anonymized data, that is data which no longer permits identification of data subjects, is not subject to such retention periods);
(iii) Fingerprints shall not collect more data than is needed in order to be able to fulfill the task at hand, which essentially means that personal data cannot be collected because it is ‘nice to have’; and
(iv) Personal data shall be accurate and kept up to date. Inaccurate or outdated personal data must therefore either be updated or deleted from Fingerprints’ systems.
6 COMMUNICATING PRIVACY INFORMATION

When collecting personal data, Fingerprint will inform the data subjects of what Fingerprint wants to do with their data through an appropriate privacy notice. The notice must answer the following questions:

(i) What information is being collected?
(ii) Who is collecting it?
(iii) How is it collected?
(iv) Why is it being collected?
(v) How will it be used?
(vi) Who will it be shared with?
(vii) What will be the effect of this on the individuals concerned?
(viii) Is the intended use likely to cause individuals to object or complain?
(ix) How long it is going to be retained?
(x) Will the data be transferred outside the EU/EEA area?

7 THE USE OF PERSONAL DATA

7.1 The use of personal data within Fingerprint

As the correct use of personal data is of outmost importance for Fingerprint, it will be the responsibility of every employee to ensure that it is used and stored correctly. Personal data can only be used for the reasons it was collected and by the staff that need it in order to fulfill their professional duties. The data may only be stored at its designated place within Fingerprint. If there is a need to use or store data in a new way, this must then first be approved by the DPO. For more detailed information how personal data can be used within Fingerprint, please check the appropriate guidelines.

7.2 Biometric data

In order to use biometric data, Fingerprint must have the consent from the data subject. As this data is deemed to be sensitive, Fingerprint must be sure that the biometric data that has been collected is being processed in a secure manner and not misused in any way. Please remember that consent can be withdrawn at any time, therefore treat the biometric data accordingly.

It is therefore the duty of every employee to be aware when she or he is processing biometric data that she or he is following the security measures that have been put in place. Every employee must follow the guidelines set up by Fingerprint and consult with the DPO if she or he is uncertain about the processing.

7.2.1 The collection of biometric data from employees

Fingerprint encourage all employees within the Company group to take active part in this work, and one way of doing so is to allow Fingerprint to collect certain biometric data for research purposes.

Such collection will only be carried out in relation to employees wanting to participate in the research, and who have provided their explicit consent to the collection and processing of their biometric data and other personal data related thereto.

Please note that it is completely up to the individual, as an employee, to decide whether he or she wants to help Fingerprint in this effort and provide his or her consent to the collection and processing of biometric data for this purpose.
7.3 Employee personal data

As an employer, Fingerprints will collect and process personal data for recruitment, the performance of the employment contract, diversity, health and safety. The legal ground for such processing will be the contractual necessity (e.g. for the processing of employee payment data), a legal obligation (e.g. for the processing of employee data in relation to social security) or the legitimate interest of the employer (e.g. in the context of employee monitoring).

7.4 Business contacts

Fingerprints holds information about its customers, prospects and suppliers. When such information relates to an individual it is considered personal data. It is therefore important that our business contacts will be informed about the relevant privacy notice.

8 DATA SUBJECTS’ RIGHTS

Data subjects have certain rights under the GDPR that we will respect. Fingerprints will therefore have well-defined documentation on how to provide processes in order to ensure that this is possible.

An example of a right is that when a data subject requests that any information held on them is deleted or removed (also known as “the right to be forgotten”). This right is however not an absolute right, as compliance with other legal requirements than the GDPR may require Fingerprints to keep the personal data, such as legislation concerning accounting. Fingerprints must therefore have well-defined documentation on how to provide processes to enable the possibility to erase the data at the right time that it should be removed.

9 BIG DATA ANALYTICS AND PROFILING

Big data analytics and profiling refer to processes by which large amounts of (personal) data of individuals are collected and this data are analyzed and combined to find certain (inter)relations and patterns by using complicated algorithms. The result of such analysis (profiles) is typically applied to (groups of) individuals to categorize them and/or to predict their behavior.

Many instances of big data analytics do not involve personal data at all. However, there are many examples of big data analytics that do involve processing personal data. Where we at Fingerprints use personal data, we must ensure that we are complying with our obligations under the GDPR as outlined in this document.

Each initiative with big data management must be reviewed and data analyzed, classified and received a “go ahead” from the DPO prior to be started.

10 COMPLIANCE WITH GDPR

According to the GDPR, controllers must demonstrate compliance. This means that Fingerprints is required to:

(i) Maintain records of processing activities under its responsibility. These records contain information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant,
(ii) Conduct a data protection impact assessment (DPIA) where there are increased risk of leakage or on more sensitive data – ensure that the DPO is informed, and
(iii) Implement data protection by design and by default, e.g. data minimization. A DPIA is typically required in high-risk situations, for example where new technology is being deployed or where a profiling operation is likely to significantly affect individuals.
11 CYBER SECURITY AND DATA BREACHES

Fingerprints must protect the personal data stored on its systems against unauthorized or unlawful processing and against accidental loss, destruction or damage, by ensuring that appropriate technical or organizational measures are in place to detect, report and investigate a personal data breach.

Fingerprints must also be prepared to report to the relevant Data Protection Authority where a breach has happened. Reporting must be done within 72 hours of awareness.

In order to prevent data breaches, the following applies:

(i) In cases when data is stored on printed paper, it should be kept in a secure place where unauthorized personnel cannot access it
(ii) Printed data should be shredded when it is no longer needed
(iii) Data stored on a computer should be protected by strong passwords.
(iv) Data stored on CDs or memory sticks must be locked away securely when they are not being used, for guidance read the IT policy
(v) DPO must approve any cloud used to store data
(vi) Servers containing personal data must be kept in a secure location, away from general office space
(vii) Data should be regularly backed up in line with the company’s backup procedures. Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
(viii) All servers containing sensitive data must be approved by Fingerprints IT department and protected by security software and strong firewall.

12 INTERNATIONAL TRANSFERS

When Fingerprints shares personal data with a company outside the EU/EEA, for example another group company, a service provider or a business partner, it must ensure that the receiving company has an adequate standard of data protection. This can be done by the use of the standard contractual clauses adopted by the EU Commission, relevant Data Processing Agreements (DPA) and/or Data Transfer Agreements (DTA) depending on the use and processing of the personal data.

12.1 Outsourcing and cloud services

In certain situations, there might be a need to outsource certain services. If a service includes the disclosure of personal data to third parties, such as IT service providers and cloud service providers, there must be a valid data processor agreement set in place prior to the start of using these services. As an employee, you must ensure that the DPO has been consulted in the process setting up the outsourced service.

13 CONSEQUENCES OF FAILING TO COMPLY

Fingerprints take compliance with this policy very seriously. Failure to comply puts both you and Fingerprints at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures, which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.
14 PRIVACY ORGANIZATION

In order to implement the compliance requirements under the GDPR and other applicable data protection legislation, Fingerprints will establish a steering committee headed by the DPO and with representatives from Legal, IT and HR.

The implementation of the regulation is executed as a global program and various minor projects. The monitoring of continuous compliance will be under the responsibility of the DPO for the entire Group.

14.1 DPO responsibilities

The DPO will be responsible for the following tasks within Fingerprints:

- Developing and maintaining an educational program for all Fingerprints employees concerning GDPR;
- Ensuring that data privacy is respected within Fingerprints by ensuring that policies and instructions are up to date and are in line with GDPR;
- Ensuring that data privacy practices are included within Fingerprints general Corporate Responsibility practices for all areas, unless specific GDPR legal requirements states otherwise;
- Updating the organization on the development of data privacy legislation and the interpretation of GDPR; Ensure that staff process personal data in a correct and lawful manner and are able to answer questions from potential users; and
- Ensuring that privacy impact assessment (PIA) are done in product development process and when implementing new IT systems;
- Acting as internal auditor, pointing out non-conformities and deficiencies to Information owner;
- Inform the board of any misuse of personal data within the organization.

14.2 Information owner responsibilities

The information owner is responsible for the information and thus the usage of information. Defining:

- Roles and accesses
- What the information may be used for
- To which systems/parties info is shared and what info is shared
- What information should be collected
- When the information should be deleted
- Govern that the information is correct
14.3 System owner responsibilities

The system owner owns the system and the security around it:

- Conduct security assessment
- Perform risk analysis
- Make sure that the appropriate security measures are taken and upheld
- Ensure that only the persons that have been given access to use the information can access it
- Make sure that the system can delete the information
- Ensure that there is an easy procedure set in place that enables the system to extract personal data in accordance with a demand for access by an individual
- Make a map over how personal data enters into the system, how it leaves the system, how the system interacts with other systems

14.4 Who is responsible for this policy?

All policy documents are approved by the Management Team and the Board of Directors. This policy is owned by the General Counsel, who stipulates its content. The DPO is responsible for its execution.