PRIVACY POLICY

This Privacy Policy explains how Facepoint collects, processes, discloses, stores, and protects information about heightened-risk individuals in connection with our Service or Database. It also provides information about heightened-risk individuals' rights and how any individual can contact us if he or she has any questions about how we handle heightened-risk individuals' information.

1. Context

Faced with the obligation to monitor their current and potential customers under the "Know Your Customer" in the context of the fight against money laundering and terrorist financing (hereinafter, "AML/CFT"), the organizations and institutions subject to the obligations in this respect (hereinafter, the "Reporting Institutions") have an undertaking to verify the identity of customers and identify those who pose a risk. Facepoint responded to this requirement by offering a service for identifying the heightened-risk individuals.

2. Scope, sourcing and coverage

All data included in our Database comes solely from publicly available information, including photographs. Facepoint relies on Open Sources Intelligence research methods, defined by NATO as the use of "unclassified information that has been deliberately discovered, analyzed, extracted and disseminated to a selected group in order to answer a specific question". This includes data that have been "manifestly made public" by the data subjects and data published by private or public bodies and present on the Internet, such as lists of international sanctions or reports of judgments and sentences, etc. A valid and public URL is attached to each photograph collected.

The data are specifically derived from the following sources: official sanctions lists, lists published by police agencies or law enforcement bodies, as well as by administrative authorities; official websites of governments and international organizations; public court documents; company websites; international, national and local media deemed reputable and credible; other data clearly made public by concerned parties.

Heightened-risk individuals are defined according to the following categories:

- "politically exposed person" ("PEP"): within the meaning of the FATF Recommendations which are global standards against money laundering and terrorist financing issued by the Financial Action Task Force on Money Laundering (FATF), an inter-governmental body originally created by the G7 in 1989 and currently has approximately 40 members;
- Sanctions: an individual who is listed on the website of a regulatory, law enforcement or government agency (e.g. Interpol) in relation to money laundering, terrorist financing, corruption or similar activities as defined by the FATF; of a government or international organization (for example, the sanctions lists published by the European Union);
- Persons of Interest (Terrorism, Organized crime, Financial crime): an individual is linked to terrorist or financial crime activities ; or an individual has been charged, investigated, arrested, charged or convicted of crimes that are a possible prerequisite for money laundering or

terrorist financing (e.g., arms trafficking, smuggling, fraud, membership in an organized crime group, environmental offences, war crimes), that are also listed by the FATF as being at risk, or is suspected of participating in these activities.

The inclusion of information about heightened-risk individuals in our Database does not automatically mean that they are involved in or linked to financial crime, terrorism or any other criminal or illegal act. For example, being identified as a PEP simply indicates to a Facepoint client that an individual holds, or has held, a prominent political or public office.

Facepoint's customers must make their own decisions about how to use the data provided to inform their due diligence activities, carrying out their own independent assessments to verify the veracity of information.

3. Categories of personal data

The Database contains photographs and web links of open access sites on which these data were collected; Identity data (surname, first name, name in original script in cases of a language in a non-Latin alphabet, alias, gender, date of birth, country of residence); titles/functions and activities (current and past); data on the existence of criminal prosecutions and convictions ; the fact that the person is deceased if the information comes from an official source; if applicable, links to other heightened-risk individuals, businesses, associations or organizations.

Personal data on Facepoint may be "sensitive" or "special categories" of personal data, such as: information about heightened-risk individuals' political views (for example, if they are a PEP holding a position in a political party); information about their racial or ethnic origin (for example, if it can be reasonably inferred from other information about them on our Database, such as their name, location, citizenship, or photograph). Under no circumstances, however, is this information the subject of a data field within the Database; or biometric data, calculated from publicly available photographs of heightened-risk individuals.

Emphasis should be placed on the care that is taken to collect only reliable data through a manual verification process that is carried out by Facepoint analysts with the technical aptitude, training and expertise to do so. Only data relating to heightened-risk individuals that are truly "adequate, relevant and limited to what is necessary for the purposes for which they are processed", within the meaning of Article 5(c) of the General Data Protection Regulation (hereinafter, the "GDPR"), are recorded in the Database.

4. Purposes of processing

If heightened-risk individuals' information is included in Facepoint, it is processed (e.g., collected, used, shared and retained) only for the purpose of:

- allowing our customers to perform their due diligence;
- processing requests on the Database;
- Responding to requests from courts, law enforcement agencies, regulatory bodies and other public and governmental authorities;
- Exercise our rights, defend against claims and comply with the laws and regulations that apply to Facepoint or third parties we work with;
- Receiving the services from our professional advisors, such as lawyers, accountants, consultants or information security professionals;
- Protecting our rights.

5. Legal grounds for processing

We process standard personal data on the basis that it is necessary for the purposes of our legitimate interests and those of our customers. We only process special categories of data that have been manifestly made public by the data subject, again because it is necessary for the purpose of our legitimate interest.

A legitimate interest is pursued by a Reporting Institution that follows reasonable and proportionate procedures - in accordance with non-binding guidelines of the relevant public financial supervisory authority - to verify the identity of any person wishing to open an account. The legitimate interest pursued by a third party as a legal basis for the processing includes situations where the controller assists private actors in their fight against illegal activities, such as money laundering.

It is in the interest of Reporting Institutions to comply with the legal obligations to which they are subject in the context of the AML/CFT legal framework. The interest of the Reporting Institutions is real, present and imperative. It benefits society in general as soon as it contributes in particular to the fight against money laundering and terrorist financing.

6. Recipients of the data

Information within our Database is intended for our customers, third parties who provide us with advice and services, and business partners who work with us to make Facepoint data available. Our third-party service providers are not allowed to share or use the personal data we make available to them for any purpose other than to provide services to us. We also disclose information about heightened-risk individuals to relevant authorities (including any national and/or international regulatory or law enforcement agencies or other form of tribunal) when we are required to do so or at their request.

7. Security Measures

We undertake to take all useful precautions to preserve the security of both Users' and heightened-risk individuals' personal data, and in particular to prevent them from being distorted, damaged or communicated to unauthorized persons. We implement the following security measures among many others:

- Physical security measures,
- An authorization management system that limits access to the premises and to our information system to only those people who need to access them in the context of their functions and scope of activity,
- Authentication processes for users and administrators,
- Within the framework of support and maintenance operations, an authorization management system,
- Processes and devices that allow the tracing of all the actions carried out on our information system, and to carry out, in accordance with the applicable regulations, reporting actions in case of an incident impacting the data.
- monitoring compliance with our policies, procedures and controls.

It is specified that our Customers ensure the security of the resources, systems and applications that they implement while using our Services, and remain responsible for the implementation of systems such as firewalls, the updating of deployed systems and software, the management of access rights, the configuration of resources, etc. We also impose contractual restrictions on our customers and

business partners, requiring them to use the Facepoint Database only in connection with their legal or regulatory due diligence obligations.

8. International Transfers

The personal data Facepoint processes, as a Controller or as a Processor, are located in countries offering an adequate level of protection either because they comply with the provisions of the GDPR or the amended French "Data Protection Act", or because they are recognized as adequate by the European Union (hereinafter, "EU"). In the event that Facepoint or one of its subcontractors transfers personal data to countries that do not offer levels of protection that are not equivalent to the level of protection of personal data in the EU, Facepoint undertakes to ensure that such transfer is governed by the signature of Standard Contractual Clauses established by the European Commission.

In the event that personal data stored by the Reporting Institutions are transferred to a country of destination considered by the European Commission as not providing a sufficient level of protection of personal data, one of the guarantee mechanisms recommended by the European Commission such as Standard Contractual Clauses or any other protection mechanism in compliance with the applicable regulations will be put in place, as a contractual requirement.

9. Retention periods

The retention periods differ according to the category of heightened-risk individuals concerned. Thus, it is specified that the retention periods for data of suspected persons must be different from those relating to convicted persons. Indeed, if the retention of private data does not amount to the expression of suspicion, the conditions of such retention must not give them the impression that they are not considered innocent.

We calculate the retention period of heightened-risk individuals' personal data according to the following criteria:

- the length of time heightened-risk' individuals personal data remains relevant to the screening process;
- the length of time it is reasonable to keep records to demonstrate that we have fulfilled our duties and obligations;
- the limitation periods within which claims may be made;
- any retention period prescribed by law or recommended by regulatory authorities, professional bodies or intergovernmental associations or organizations;
- the existence of any relevant procedures.

10. Data subjects' rights

Heightened-risk individuals have the right, under European laws in particular, to access their personal data and to ask us to correct, delete and restrict the use of their information. Heightened-risk individuals may also have the right to object to the use of their personal data.

We will respect all of heightened-risk individuals' rights under applicable data protection laws. Heightened-risk individuals have the following rights under European laws regarding personal data processed by Facepoint:

Right to be informed: the right to be informed of what we do with their personal data; this is the very purpose of this privacy statement.

Right of access: The right to request in writing details of their personal data and a copy of the personal data we hold about them.

Right to object: The right of opposition allows an individual to object to his/her data being used by an organization for a specific purpose. The individual must put forward "reasons relating to his/her particular situation"

Right of rectification and erasure: The right to have inaccurate information about heightened-risk individuals corrected or deleted.

There are limits to the rights heightened-risk individuals have with respect to their personal data and, in certain circumstances, we may not be required or able to respond to a request, or we may only partially respond to a request. In such cases, we will provide heightened-risk individuals with an explanation of the legitimate reasons why we are unable or not required to respond to their request.

11. Contact

If an individual has any questions, comments, complaints or suggestions regarding data protection or this Privacy Statement, or any other concerns about the way Facepoint handles information about heightened-risk individuals, they may contact our privacy team at dpo@facepoint.co.

Facepoint may modify or amend this privacy statement from time to time. Any future changes or additions to the processing of personal data as described in this privacy statement affecting any heightened-risk individual will be communicated through an appropriate channel.