Notice concerning the protection of personal data for (Professional Customers)

This document is a general Description of how POST Processes Personal Data as Processor, according to the instructions of its Customer.

GENERAL DESCRIPTION

DEFINITIONS

"**Agreement**": the contract concluded between POST and its Customer in the context of which POST processes Data on behalf of the Customer and according to his/her/its Instructions;

"**Controller**": 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 and gives Instructions to the Processor. In the present case, the Controller is the POST Customer;

"**Customer**": any professional customer of POST as defined in the POST General Terms and Conditions;

"**Description(s)**": the General and/or Specific Description;

"**General Description**": a general overview of the Data Processing performed by POST as Processor of the Customer, on the Customer's Instruction and in the context of its contractual customer relationships. The Descriptions (General and Specific) may be subject to any revisions required by the Law;

"**Specific Description**": a detailed overview of the Customer's written Instructions regarding the Processing performed by POST as Processor of the Customer, as set out in a contract, the terms and conditions, a subscription form or any other document identified as such;

"**Personal Data**" **or** "**Data**": the personal data, as defined by Law, provided by the Customer as Controller and processed by POST as Processor (e.g. name, address [physical and email], telephone number, account number, etc.);

"**Instruction(s)**": the written and documented instructions issued to the Processor by the Controller, defining terms and conditions for Data Processing;

"**Law**": all laws, regulations and other requirements applicable in the Grand Duchy of Luxembourg, in particular relating to Data protection, the protection of privacy, electronic storage, confidentiality or Personal Data, including the General Data Protection Regulation (Regulation EU 2016/679) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;

"**Notice**": the General Description and, where appropriate, the Specific Description(s);

"**Person(s) Concerned**": any identified or identifiable natural person whose Data is subject to Processing;

"**POST**": POST Telecom S.A., having its registered office at 1 rue Emile Bian, L-1235 Luxembourg, registered with the Luxembourg Trade and Company Register under number B 43290;

"**Processing**": any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

"**Processor**": a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller and according to his/her/its Instructions. In the present case, the Processor is POST;

"**Security Incident**": any of the following incidents, actual or suspected: (i) accidental or unlawful destruction, loss or theft of Personal Data; (ii) unauthorised use, disclosure, acquisition, alteration, transmission, access, or any other unauthorised Processing of Personal Data that may reasonably compromise the privacy or confidentiality of the Personal Data; or (iii) inability to access the Customer's or Processor's systems, which may be caused by a malicious infection of these systems and which may reasonably compromise the privacy or confidentiality of Personal Data. Security Incidents thus include, without limitation, ransomware attacks, distributed denial-of-service attacks or any other similar incidents whereby a third party obtains control over the Controller's/Processor's systems or otherwise prevents the Controller/Processor from performing lawful Data processing.

1. Customer's obligations

In the context of their contractual relationships, the Customer, as Controller, and POST, as Processor, undertake to comply with the Law.
The Customer has primary responsibility for ensuring the legality of Processing activities. Therefore, the Customer undertakes to:

(i) provide POST with clear and sufficiently documented Instructions in the Specific Description;
(ii) keep a register of the Processing activities under his/her/its responsibility;
(iii) implement technical and organisational measures to ensure a sufficient level of protection for Personal Data. In so doing, the Customer shall take into account the nature, scope, context and goals of the Processing as well as the risks of adverse impacts on the rights and liberties of the Person Concerned. These measures shall be reviewed and adapted as necessary;
(iv) respect the rights of the Person Concerned;
(v) obtain the approval of the relevant control authorities where required;
(vi) notify Security Incidents to the relevant control authority in accordance with the provisions of the Law.

2. Obligations of POST

To the extent that performance of the Agreement requires POST to perform Personal Data Processing operations, POST will act exclusively on behalf of the Customer and according to his/her/its Instructions and shall:
(i) respect the strict confidentiality of Personal Data;
(ii) impose a confidentiality obligation on staff responsible for performing operations on the Data;
(iii) ensure the security of Personal Data processed in accordance with paragraph 8 below;
(iv) inform the Customer regarding POST processors involved in the Processing operations;
(v) implement reasonable measures, proportionate to its level of involvement in the Processing, in order to assist the Customer when he/she/it is replying to requests from the Persons Concerned;
(vi) delete or provide access to Personal Data, depending on the Customer's decision, at the end of the contractual relationship in the context of potential reversibility;
(vii) provide the Customer with all information necessary in order to demonstrate compliance with legal obligations (this especially includes the register of categories of processing activities performed by POST on behalf of the Customer).

Should POST reasonably consider an Instruction to be in breach of the Law, it shall inform the Customer immediately.

3. Confidentiality

POST processes Personal Data as confidential information.

POST undertakes not to disclose Personal Data to any third party, as specified by the Law, except in accordance with the Customer's Instructions or under other obligations specified in Law or imposed by any other relevant control authority or court decision, in which case it shall (i) make all reasonable efforts to advise the Customer prior to this disclosure and, in all cases, immediately following it and (ii) take all possible measures to limit the disclosure of Personal Data to that which is strictly necessary in order to meet this obligation.
POST will strive to impose confidentiality obligations on any staff members responsible for processing Personal Data, as well as on its own processors, where appropriate.

4. POST subcontractors

POST will not subcontract any Customer Data Processing operations without first informing the Customer.
Where POST uses subcontractors to assist it in performing Data Processing operations, POST shall ensure that these subcontractors are contractually bound to maintain appropriate guarantees for the Processing of this Data in accordance with the Law.

5. Security

POST implements a reasonable set of technical and organisational measures in order to ensure a level of security for the Data and/or Customer Data Processing that is appropriate to the risks identified.

The security measures are intended to protect Personal Data from destruction or accidental or unlawful loss, alteration, unauthorised disclosure or access. For example, categories of measures might include:

- human resource security;
- security and data protection awareness and training programme;
- secure media handling (storage, transfer and disposal);
- logical access control;
- physical and environmental security;
- cryptography;
- IT service management processes (Security Incident management, change management, etc.);
- separation of development, testing and operational environments;
- protection of test data;
- malware protection;
- backups;
- logging and monitoring;
- technical vulnerability management;
- network security;
- system acquisition, development and maintenance;
- compliance and security audit.

6. Security Incident response and notification

Should Personal Data be compromised, the Party becoming aware of the fact shall notify the other party by the fastest means possible, within a maximum of 72 hours of becoming aware of it. The Parties undertake to provide each other with mutual assistance in informing the relevant control authority that this Personal Data has been compromised.

7. Deletion of Personal Data

Unless otherwise provided by Law or unless a reversibility service has previously been negotiated in the Agreement, POST undertakes to delete all Customer Personal Data definitively upon expiry of the Agreement.

8. Rights of the Persons Concerned

POST will give the Customer proportionate assistance regarding the answers that should be given in response to requests from the Persons Concerned, for each category of Processing operation performed on behalf of the Customer.

The provisions of the General and Specific Descriptions survive the termination of the Agreement.