Data Protection Agreement

Introduction

As the Service Provider may process Personal Data under the scope of the commercial relationship with its Clients. The purpose of the Charter is to set out the rights and obligations of the Parties.

1. Definitions

In this Charter, the words and expressions starting with a capital letter have the following meaning:

- "**Charter**" means the present document.
- **"Personal Data or PD"** means any information relating to a natural person identified or who can be identified (hereinafter the "Data Subject"), directly or indirectly, particularly in reference to an identification number, location data, online identifiers (for example, pseudonyms and passwords) or one or more elements specific to their physical, physiological, mental, economic, cultural or social identity;
- **"Regulations"**: means all the laws and regulations applicable in the European Union regarding PD, including the French "Data Protection" law no. 78-17 dated 6 January 1978, amended, and the General Data Protection Regulation on Personal Data 2016/679 dated 27 April 2016.
- "**Services**" means all the services carried out by the Service Provider for its Clients.
- "**Controller**" means the natural person or legal entity, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing. Under the framework of the Services carried out by the Service Provider, the Controller is the Client.
- "**Processor**" means the natural person or legal entity, public authority, agency or other body which processes PD on behalf of the Controller and according to its instructions. Under the framework of the Services carried out by the Service Provider, the Processor is the Service Provider.
- "**Processing**" means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as the 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;
- The terms and expressions **"PD breach", "Process", "Data Subject", "Member State", "Supervisory Authority", "Standard Clauses",** have the same meaning as the one given in the Regulations, and closely related expressions must be interpreted in the same manner.

2. General obligations of the Client

The Client undertakes to respect the Regulations.

The Service Provider will only process Personal Data after receiving documented instructions from the Client and exclusively to carry out the Services.

If the Client uses the Services that are the purpose of the Contract to process other data or categories of Personal Data or for other types of Processing, the Client will do it at its own risk and the Service Provider will not be held liable for any breaches of the Regulations.

The Client, as the Controller, undertakes to notify the Service Provider immediately in the event of any changes to the Services requested, resulting in or which may result in a potential change to the Processor status of the Service Provider with regard to the Regulations.

The Client recognises that the undertakings of the Service Provider set out in this Charter provide sufficient guarantees regarding the compliance of the Service Provider to the Regulations.

The Client recognises that the processing of the Service Provider is limited to following documented instructions of the Client, and that it will notify the Client when any instructions given breach the Regulations. Any instruction not documented in writing or that is non-compliant with the Regulations will not be taken into account.

The Client will keep a register or all processing operations it performs as the Controller. As a minimum, this register will contain the mandatory information required by the Regulations.

The Client is responsible for providing information to the data subjects concerned by the processing when collecting PD. As determined by the Controller, the Service Provider will help the Client implement this disclosure obligation. In such cases, the terms and conditions of the assistance requested by the Client shall be agreed mutually between the Client and the Service Provider.

3. Obligations of the Service Provider to the Client

✓ Acting on the basis of documented instructions of the Controller

The Service Provider undertakes to process the Personal Data that are the subject of this Charter in accordance with the instructions, unless the Service Provider is obliged to process the PD by virtue of a mandatory provision stemming from community law or from the laws of the Member State to which it is subject. In such cases, the Service Provider will inform the Client in a timely fashion and, wherever possible, before the Processing.
If the Service Provider considers that an instruction breaches the Regulations, the Service Provider undertakes to inform the Client.

✓ Guaranteeing the confidentiality of PD

The Service Provider undertakes to guarantee the confidentiality of Personal Data processed.

The Service provider undertakes to ensure that the persons authorised to process Personal Data:

- Undertake to respect the confidentiality or are subject to an appropriate legal confidentiality obligation;
- Receive the necessary awareness training on the protection of Personal Data.

✓ Subcontracting

The Service Provider may use another subcontractor ("Subsequent subcontractor") to carry out specific processing activities. In such cases, it will inform the Client in writing. The Client has a period of five (5) working days to express any reservations.

It is up to the Service Provider to ensure that the Subcontractor offers sufficient guarantees in terms of the implementation of appropriate technical and organisational measures to guarantee that the Processing meets the requirements of the Regulations.

✓ Rights of individuals

To the extent possible, the Service Provider will help the Client to fulfil its obligation to follow up requests by data subjects to exercise their rights under the Regulations, namely: the right of access, rectification, erasure and opposition, right to the restriction of processing, right to the portability of PD, and rights to not to be the subject of automated individual decision making (including profiling according to the meaning of the Regulations).

When data subjects send requests to the Service Provider in relation to the exercising of their rights, the Service Provider will send these requests by e-mail to the person designated by the Controller or communicated by any other means. The Service Provider may only respond directly to requests from a data subject after receiving a documented instruction from the Controller.

The Client acknowledges that the aforementioned steps fulfil the cooperation and assistance obligation of the Service Provider towards the Client to enable it to ensure that the Processing complies with the Regulations. If additional due diligence requirements are necessary, the Parties agree to meet and discuss in good faith the conditions of these additional requirements.

✓ Notification of Personal Data breaches

A Personal Data breach is understood as any security breach resulting, accidentally or unlawfully, in the destruction, loss, alteration or unauthorised disclosure of PD transmitted, stored or otherwise processed, or the unauthorised access to such PD.

The Service Provider will notify the Client of any Personal Data breaches as soon as possible after discovery the breach and in accordance with the procedure defined by the Controller unless the breach in question is not likely to result in any breach of the rights and freedoms of individuals. This notification should be accompanied by any appropriate documents to allow the Controller, if necessary, to inform the competent supervisory authority of the breach.

The Client acknowledges that the aforementioned steps fulfil the cooperation and assistance obligation of the Service Provider towards the Client to enable it to ensure that the Processing complies with the Regulations. If additional due diligence requirements are necessary, the Parties agree to meet and discuss in good faith the conditions of these additional requirements.

✓ Impact assessments

The Service Provider will help the Controller conduct any data protection impact assessments it may decide to perform.

The Client acknowledges that the aforementioned steps fulfil the cooperation and assistance obligation of the Service Provider towards the Client to enable it to ensure that the Processing complies with the Regulations. If additional due diligence requirements are necessary, the Parties agree to meet and discuss in good faith the conditions of these additional requirements.

4. Security and confidentiality obligation

The Service Provider undertakes to implement all appropriate technical and organisational measures and to take all due care to ensure a level of security adapted to the existing risk.

The Service Provider undertakes to take all necessary steps in view of the nature of the Data and the risks involved in the Processing to preserve the security of the Data and prevent any deformation, alteration, damage, destruction, in a fortuitous or unlawful way, loss, disclosure, and/or any access by unauthorised third parties.

The measures taken by the Service Provider must take into account the most recent technical functionalities and the cost of their implementation, as well as the characteristics of the processing (nature, scope, purpose, etc.) and the risks involved for the rights of the Data Subjects. These may include:

- ✓ data encryption measures;
- ✓ measures that guarantee, during the implementation of the processing, the confidentiality, integrity, availability and resilience of the systems and services used to process the data;
- ✓ measures to restore access and availability of data as quickly as possible in the event of any equipment or technical incidents;
- ✓ procedures to evaluate and test the effectiveness of technical and organisational measures.

The Client acknowledges that the aforementioned steps fulfil the cooperation and assistance obligation of the Service Provider towards the Client to enable it to ensure that the Processing complies with the Regulations. If additional due diligence requirements are necessary, the Parties agree to meet and discuss in good faith the conditions of these additional requirements.

5. Return or deletion of Personal Data

At the end of the Contract, the Service Provider must, as determined by the Client, either return all the Personal Data processed, or delete the data and confirm to the Client in writing that such data has been deleted, subject to and within the limits of the legal and regulatory storage obligations imposed upon the Service Provider.

6. Audits

The Client may, if it wishes, within the limit of one (1) time per year, perform, at his own expense, an audit within Service Provider's premises, directly or through any independent third party, no competitor of the Service Provider, in order to ensure compliance with the protection measures of the DP, processed within the framework of the Services.

In the event that the Client wishes to call on a third party to carry out the audit, the latter expressly undertakes to have said third party sign a confidentiality agreement and to make sure that its terms are respected.

The Client will notify the Service Provider with at least forty (45) calendar days' notice, any request for an audit operation, the date of the audit as well as the name of any third party in charge of the audit. The Service Provider may refuse the audit firm and the persons designated to perform the audit, if the client's proposal reveals a conflict of interest and / or if the audit firm is a competitor of the Service Provider. In case of refusal, the Service Provider must notify it within eight (8) calendar days following the notification of the audit made by the Client or by an audit firm in charge of carrying it out (the Auditor) under the conditions defined in this Charter.

The arrangements for carrying out the audit will be the subject of a prior agreement signed by the Parties, which will include the following conditions:

- Audit schedule, being specified here that the audit will be able to be held only days and hours worked
- Stakeholders involved
- The qualities of the audit firm and the auditor, being specified here that the audit firm and the auditor will have to be certified ISO 27 001 and / or GDPR compliant
- How to communicate the audit report to the Service Provider
- The procedures for implementing a corrective action plan resulting from the aforementioned audit report.

The Service Provider will cooperate in good faith with the Auditor and will communicate to him any information or documents or explanations necessary for carrying out the audit. The access procedures will be communicated by the Service Provider to the Client who must respect them. Logical connections to access Client's data will be made by the Service Provider at the request of the Auditor and, where necessary, in the presence of the Auditor.

The Service Provider will cover the time spent by its staff for the purposes of the audit within one (1) day per year. The audit report will be sent free of charge to the Service Provider by the auditors or by the Client, within a period defined in the audit agreement, so that the latter can formulate, within twenty (20) working days following the date of its communication, any observations or objections by registered letter with acknowledgment of receipt addressed to the auditor and the Client.

This audit report is confidential.

In the event that the audit report reveals a breach of an essential obligation relating to PD, directly and exclusively attributable to the Service Provider, the Service Provider expressly undertakes to implement at its own expense all necessary corrective measures.