**Data Processing Annex**

This Data Processing Annex is an annex to the agreementbetween [Supplier Contracting Entity] [acting on its own behalf and in the name and on behalf of each Supplier Affiliate] ([collectively] “**Supplier**”) and Marionnaud Lafayette (“**Marionnaud**”) (the “**Agreement**”).

### In consideration of Marionnaud making the Marionnaud Personal Data available to the Supplier, the Supplier hereby agrees to process the Marionnaud Personal Data in accordance with the terms and conditions of this Data Processing Annex (the “**Annex**”).

**SUMMARY**

SECTION I - GENERAL PROVISIONS

Clause 1. Purpose and scope

Clause 2 : Invariability

Clause 3 : Interpretation and hierarchy

## SECTION II - OBLIGATIONS OF THE PARTIES

Article 4 : Instructions

Clause 5 : Purpose limitation

Clause 6 : Secondary processing

Clause 7 : Processing duration

Clause 8 : Sensitive data

Clause 9 : Documentation and compliance

Clause 10 : Access requirements

Clause 11 : Use of Sub-Processors

Clause 12 : International data transfers

Article 13 : Assistance

Clause 14 : Public access notification

Clause 15 : Security of processing

Clause 16 : Data breach notification

Clause 17 : Data breach by Marionnaud

Clause 18 : Data breach by the Supplier

SECTION III – FINAL PROVISIONS

Clause 19 : Non-compliance and termination

Clause 20 : Deletion or return of personal data

Clause 21 : Indemnity

APPENDICES

Appendix I – List of parties

Appendix II – Description of processing

Appendix III – Appropriate technical and organisational measures

Appendix IV – List of sub-processors

**Definitions**

Terms used in this Annex have the same meaning as those used in the Services Agreement, unless provided otherwise.

“**Affiliate**” means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with the Supplier, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

“**Appropriate Technical and Organisational Measures**” means processes and procedures which, having regard to the state of technological development, the cost of implementation, the nature, scope, context and purpose of processing of Marionnaud Personal Data, and the risks of varying likelihood and severity for the rights and freedoms of the data subjects, will ensure a level of security appropriate to the harm that might result from unauthorised or unlawful processing of, or accidental loss or destruction of, or damage to, Marionnaud Personal Data. Such measures shall comprise, as a minimum, those measures set out in Appendix III and any additional measures from time to time notified in writing by Marionnaud to the Supplier and reasonably agreed by the Parties;

“**Marionnaud Personal Data**” means any Personal Data processed by the Supplier: (i) on behalf of Marionnaud; (ii) on behalf of any client of Marionnaud, or (iii) otherwise processed by the Supplier, in each case pursuant to or in connection with instructions given by Marionnaud consistent with the Services Agreement;

“**Data Controller and Data Sub-Processor(s)**” shall have the meaning given to it in the relevant Data Protection Laws;

“**Data Protection Laws**” means:

(a) in EU/EEA countries, all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the EU/EEA Member States, including the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (the “GDPR”);

(b) in Switzerland, all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in Switzerland, including the Federal Act on Data Protection of 19 June 1992 (SR 235.1, the “FADP”) and the revised version of the FADP of 25 September 2020 that is scheduled to come into force on 1 January 2023;

(c) in the United Kingdom of Great Britain and Northern Ireland (the “UK”), all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the United Kingdom General Data Protection Regulation (the “UK GDPR”) and the Data Protection Act of 2018;

### (d) in other countries not covered above, any similar or equivalent laws, regulations or rules relating to the protection of Personal Data;

### (e) any enforceable guidance and codes of practice issued by any local regulatory authority responsible for administering Data Protection Laws; and/or

### (f) any amendments, re-enactments or changes to the items described in (a) to (e) above, from time to time;

“**Data Breach**” means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to Marionnaud Personal Data;

“**International Data Transfer**” means a transfer of or remote access to Marionnaud Personal Data out of a Non-Adequate Country;

“**ISO 27001**” means ISO 27001:2013, an information security standard that was published on 25 September 2013 by the International Organization for Standardization and the International Electrotechnical Commission (as may be updated from time to time);

“**Non-Adequate Country**” means a third country that is deemed not to provide a similar level of data protection as the one envisaged in the applicable Data Protection Laws;

“**Personal Data and Sensitive Data**” shall have the meaning given to it in the relevant Data Protection Laws ;

“**Services**” means the services provided by the Supplier in relation to the processing of Marionnaud Personal Data as described in the Services Agreement (as may be amended from time to time).

**“Supplier's Personnel”** means the representatives, employees, agents and co-contractors of the Supplier.

## **SECTION I - GENERAL PROVISIONS**

Clause 1: Purpose and Scope

(a) The purpose of this Annex is to ensure that the contractual relationship between Marionnaud, who is the Data Controller, and the Supplier, who is the Data Processor, is in compliance with the applicable Data Protection Laws, including Articles 28(3) and (4) of the GDPR.

(b) Appendix I provides the details on the Data Controller and Data Processor, whereas Appendix II provides the details on the processing of Marionnaud Personal Data pursuant to the Annex. Marionnaud may make reasonable amendments to Appendix II by written notice to the Supplier as Marionnaud reasonably considers necessary to meet legal requirements from paragraph (a).

(c) All Marionnaud Personal Data processed by the Supplier belong to Marionnaud and the Supplier shall have no rights to them.

(d) This Annex is without prejudice to other obligations to which the Parties are subject by virtue of Data Protection Laws, including provisions on International Data Transfers.

Clause 2: Invariability

(a) The Parties undertake not to modify this Annex, except for adding information to the Appendices or updating the information therein.

(b) This does not prevent the Parties from including the Annex to a broader contract, or from adding other clauses or additional safeguards, provided that they do not directly or indirectly contradict the Annex or detract from the fundamental rights or freedoms of data subjects.

Clause 3: Interpretation and Hierarchy

(a) Terms used in this Annex shall have the same meaning as those used in the Services Agreement, unless provided otherwise.

(b) In case of any conflicts or inconsistencies with the Services Agreement or any other agreement between the Supplier and Marionnaud existing at the time when the Annex is agreed or entered into force thereafter, the provisions in this Annex shall prevail.

(c) Where the Annex uses terms defined in the Data Protection Laws, those terms shall have the same meaning as in the Data Protection Laws.

(d) The Annex shall be read and interpreted in light of the Data Protection Laws and not in any way counter to the fundamental rights or freedoms of the data subjects.

## **SECTION II - OBLIGATIONS OF THE PARTIES**

Clause 4: Instructions

(a) The Supplier shall process Marionnaud Personal Data only to the extent, and in such a manner, as is necessary for the purpose of providing the Services pursuant to this Annex and on documented instructions from Marionnaud, unless required to do so by applicable law to which the Supplier is subject. In this case, the Supplier shall inform Marionnaud of that requirement before processing, unless the applicable law prohibits this on important grounds of public interest.

(b) Subsequent instructions may also be given by Marionnaud throughout the duration of the processing of Marionnaud Personal Data. These instructions shall always be documented.

(c) The Supplier shall immediately inform Marionnaud if, in the Supplier’s opinion, an instruction given by Marionnaud infringes any applicable laws.

c) For the avoidance of doubt, if the Supplier is unsure as to the parameters of the instructions issued by Marionnaud, it will, as soon as reasonably practicable, revert to Marionnaud for the purpose of seeking clarification or further instructions.

Clause 5: Purpose Limitation

The Supplier shall process Marionnaud Personal Data only for the specific purpose(s) of the processing, as set out in Appendix II, unless it receives further documented instructions from Marionnaud.

Clause 6: Secondary Processing

The Supplier agrees that it will not carry out further research, analysis, profiling or other processing which involves the use of any element of Marionnaud Personal Data (including in aggregate form) or any information derived from any processing of such Personal Data outside the scope of the Services and instructions received from Marionnaud.

Clause 7: Duration of Processing

Processing by the Supplier shall only take place for the duration specified in Appendix II.

Clause 8: Sensitive Data

If the processing involves the Sensitive Data, the Supplier shall apply specific restrictions or additional safeguards, such as encryption, anonymisation, hashing and separate storage etc..

Clause 9: Documentation and Compliance

(a) The Supplier shall process Marionnaud Personal Data in compliance with the Data Protection Laws and keep appropriate documentation on all processing activities carried out.

(b) The Supplier shall deal promptly and adequately with documented instructions from Marionnaud about the processing of the Personal Data in accordance with the Annex and Data Protection Laws.

(c) At Marionnaud’s request, the Supplier shall permit and contribute to audits of processing activities covered by the Annex, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, Marionnaud may take into account relevant certifications held by the Supplier. Marionnaud may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the Supplier and shall, where appropriate, be carried out with reasonable notice.

(d) The Parties shall make the information referred to in the Annex, including the results of any audits, available to the competent supervisory authority/ies on request.

Clause 10: Access Requirements

(a) The Supplier shall ensure that access to Marionnaud Personal Data is limited to duly authorized officers, employees, agents and contractors (“**Supplier’s Personnel**”) who need access to Marionnaud Personal Data to meet the Supplier’s obligations under the Services Agreement and this Annex; and as such to part or parts of Marionnaud Personal Data as is strictly necessary for the performance of the relevant Supplier’s Personnel’s duties.

(b) The Supplier shall ensure that all the Supplier’s Personnel:

1. are informed of the confidential nature of Marionnaud Personal Data and have committed themselves to confidentiality;
2. have undertaken training in the care, protection and handling of Personal Data; and
3. are aware of both the Supplier’s duties and their personal duties and obligations under the Data Protection Laws and this Annex.

(c) The Supplier shall take reasonable steps to ensure the reliability of any of the Supplier’s Personnel and Sub-Processors who have access to Marionnaud Personal Data.

Clause 11: Use of Sub-Processors

(a) The Supplier shall not subcontract any of its processing operations performed on behalf of Marionnaud in accordance with this Annex to a Sub-Processor, without Marionnaud’s prior specific written authorisation. The Supplier shall submit the request for specific authorisation at least ten (10) business days prior to the engagement of the Sub-Processor in question, together with the information necessary to enable Marionnaud to decide on the authorisation. The list of Sub-Processors authorised by Marionnaud can be found in Appendix IV. The Parties shall keep Appendix IV up to date.

(b) Where the Supplier engages a Sub-Processor for carrying out specific processing activities (on behalf of Marionnaud), it shall do so by way of a contract which imposes on the Sub-Processor, in substance, the same data protection obligations as the ones imposed on the Supplier in accordance with this Annex.

(c) The Supplier shall ensure that the Sub-Processor complies with the obligations to which the Supplier is subject pursuant to the Annex and applicable Data Protection Laws. In particular, all Sub-Processors shall provide sufficient guarantees to implement the Appropriate Technical and Organisational Measures listed in Appendix III in such a manner that the processing of Marionnaud Personal Data will meet the requirements of the Data Protection Laws.

(d) At Marionnaud’s request, the Supplier shall provide a copy of such a Sub-Processor agreement and any subsequent amendments to Marionnaud. To the extent necessary to protect business secret or other confidential information, including Personal Data, the Supplier may redact the text of the agreement prior to sharing the copy.

(e) Where the Supplier is permitted by Marionnaud to use Sub-Processors for any of its obligations under this Annex, the Supplier shall remain Marionnaud's sole point of contact for all matters falling within the scope of this Annex.

(f) The Supplier shall remain fully liable to Marionnaud for the Sub-Processor’s performance, as well as for any acts or omissions of the Sub-Processor in regard to its processing of the Marionnaud Personal Data. The Supplier agrees to notify Marionnaud of any failure by the Sub-Processor to fulfil its contractual obligations or any infringements of the Data Protection Laws with impact on the processing of Marionnaud Personal Data.

(g) Marionnaud may revoke its prior approval of a Sub-Processor where, in Marionnaud's reasonable opinion, the performance of the Sub-Processor is materially deficient, or in breach of this Annex or the applicable Data Protection Laws.

(h) The Supplier shall agree a third-party beneficiary clause with the Sub-Processor whereby - in the event the Supplier has factually disappeared, ceased to exist in law or has become insolvent - Marionnaud shall have the right to terminate the Sub-Processor’s contract and to instruct the Sub-Processor to erase or return Personal Data.

Clause 12: International Data Transfers

(a) The Supplier and any of its sub-contractors shall not transfer Marionnaud Personal Data to any Non-Adequate Country or make such Personal Data accessible from any such Non-Adequate Country without the prior written approval of Marionnaud, unless there is a specific requirement under the applicable laws binding upon the Supplier or its Sub-Processor.

 (b) In so far as there is any International Data Transfer, the Supplier and Marionnaud shall enter into a data transfer agreement containing the standard contractual clauses adopted by the European Commission in accordance with of Article 46(2) of the GDPR, provided the conditions for the use of those standard contractual clauses are met.

(c) The Supplier agrees that where it engages a Sub-Processor (including an Affiliate) in accordance with Clause 11 for carrying out specific processing activities (on behalf of Marionnaud) and those processing activities involve any International Data Transfer, the Supplier and the Sub-Processor shall enter into a data transfer agreement containing the standard contractual clauses adopted by the European Commission in accordance with of Article 46(2) of the GDPR, provided the conditions for the use of those standard contractual clauses are met.

(d) Where a data transfer agreement is to be entered into under paragraphs (b) and (c) above, the Supplier and Marionnaud (or the Supplier and its Sub-Processor, as the case may be) shall undertake a transfer impact assessment to consider the sufficiency of protections afforded in the Non-Adequate Country and implement necessary supplementary measures if required.

Clause 13: Assistance

(a) The Supplier shall promptly, and in any case within twenty four (24) hours of having been aware, notify Marionnaud of any request regarding Marionnaud Personal Data it has received from the data subject, including Marionnaud’s employee, customer or contractor. It shall not respond to the request itself, unless authorised to do so by Marionnaud.

(b) The Supplier shall assist Marionnaud in fulfilling its obligations to respond to data subjects’ requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations the Supplier shall comply with Marionnaud’s instructions.

(c) In addition the Supplier shall assist Marionnaud in ensuring compliance with the following obligations, taking into account the nature of the data processing and the available information:

1. to carry out an assessment of the impact of the envisaged processing operations on the protection of Personal Data (a ‘Data Protection Impact Assessment’) prior to processing, where a type of processing is likely to result in a high risk to the rights and freedoms of data subjects;
2. to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by Marionnaud to mitigate the risk;
3. to assist, where necessary, Marionnaud in carrying out a review to assess if the processing of Marionnaud Personal Data is performed in accordance with the data protection impact assessment, at least when there is a change in the risks represented by the processing operations;
4. to ensure that Personal Data is accurate and up to date, by informing Marionnaud without delay if the Supplier becomes aware that the personal data it is processing is inaccurate or has become outdated;
5. to ensure the level of security as required by Article 32 of the GDPR or other applicable Data Protection Laws.

Clause 14: Public Access Notification

(a) The Supplier shall promptly, and in any case within twenty four (24) hours of having been aware, inform Marionnaud if it:

1. receives an enquiry, subpoena or request for inspection or audit from a public or supervisory authority relating to processing of Marionnaud Personal Data, unless the Supplier is prohibited by law from making such notification;
2. intends to disclose Marionnaud Personal Data to any public or supervisory authority;
3. becomes aware of any direct access to Marionnaud Personal Data by public authorities in accordance with applicable laws.

The notification shall include any information that could be relevant for Marionnaud, including (if possible) details about requested or accessed Personal Data, requesting or accessing authority, legal basis and any response provided.

(b) If the Supplier is prohibited from notifying Marionnaud under the applicable law, the Supplier shall use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The Supplier agrees to document its best efforts in order to be able to demonstrate them on Marionnaud’s request and keep the evidence throughout the lifecycle of this Annex.

c) The Supplier agrees to use its best efforts to review and challenge the legality of requests coming from public authorities and provide the minimum amount of information permissible when responding to such requests, if possible in consultation with Marionnaud.

Clause 15: Security of Processing

(a) The Supplier agrees to keep Marionnaud Personal Data strictly confidential and not to use or disclose it for any purposes other than specific activities authorised pursuant to this Annex.

(b) The Supplier shall implement Appropriate Technical and Organisational Measures specified in Appendix III to ensure the security of Marionnaud Personal Data and to protect Personal Data from a Data Breach.

Article 16: Data Breach Notification

In the event of a Data Breach, the Supplier agrees to:

1. take, as soon as possible, adequate remedial measures,
2. notify Marionnaud about the Data Breach,
3. investigate and report to Marionnaud on the cause of the Data Breach,
4. cooperate with Marionnaud when developing and executing a response plan, and
5. where applicable assist Marionnaud in complying with its obligations to notify the Data Breach to the supervisory authority or data subjects in accordance with the applicable Data Protection Laws, taking into account the nature of the processing performed by the Supplier and the information available thereto.

Clause 17: Data Breach by Marionnaud

(a) In the event of a Data Breach concerning the Personal Data processed by Marionnaud, the Supplier shall assist Marionnaud in notifying the Data Breach to the competent supervisory authority/ies, without undue delay after Marionnaud has become aware of it (where relevant), unless the Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons. The Supplier shall also support Marionnaud in obtaining the following information, which shall be stated in Marionnaud’s notification:

1. nature of the Personal Data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of the Personal Data records concerned;
2. likely consequences of the Data Breach;
3. measures taken or proposed to be taken by Marionnaud to address the Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(b) The Supplier shall also assist Marionnaud in complying with the obligation to communicate without undue delay the Data Breach to the data subject, pursuant to applicable Data Protection Laws, including Article 34 of the GDPR, when the Data Breach is likely to result in a high risk to the rights and freedoms of natural persons.

Clause 18: Data Breach by the Supplier

(a) In the event of a Data Beach concerning Marionnaud Personal Data processed by the Supplier or any of its Sub-Processor(s), the Supplier shall document the Data Breach and notify Marionnaud without undue delay, and in any event within twenty four (24) hours after the Supplier or any of its Sub-Processor(s) has become aware of the breach. Such notification shall contain, at least:

1. date and time that the Data Breach occurred;
2. circumstances surrounding the breach, and any relevant facts regarding the nature and extent of the breach;
3. categories and approximate number of data subjects concerned and categories and approximate number of the Personal Data records concerned;
4. likely consequences of the breach;
5. full details of any investigation that has commenced regarding the breach (whether internal to the Supplier or external (e.g. by a regulatory body));
6. volume and details of complaints received from any individuals in respect of such breach;
7. full details of how the Supplier proposes to rectify the breach in order to mitigate its possible adverse effects; and
8. details of a contact point where more information concerning the breach can be obtained.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay, including at Marionnaud reasonable request.

(b) The Supplier and its Sub-Processor(s) shall also assist Marionnaud in complying with the obligation to communicate without undue delay the Data Breach to the data subject, pursuant to applicable Data Protection Laws, including Article 34 of the GDPR, when the Data Breach is likely to result in a high risk to the rights and freedoms of natural persons.

## **SECTION III - FINAL PROVISIONS**

Clause 19: Non-compliance and Termination

(a) The Supplier shall promptly inform Marionnaud in case it is unable to comply with this Annex, for whatever reason.

(b) Without prejudice to the Data Protection Laws, in the event that the Supplier is in breach of its obligations under the Annex, Marionnaud may instruct the Supplier to suspend processing of Marionnaud Personal Data until the latter complies with the Annex or until the Services Agreement is terminated.

(c) Marionnaud shall be entitled to terminate the Services Agreement insofar as it concerns processing of Marionnaud Personal Data in accordance with this Annex if:

1. the processing has been suspended by Marionnaud pursuant to point (b) above and the compliance with the Annex is not restored within a reasonable time, in any event within one (1) month following the suspension;
2. the Supplier is in substantial or persistent breach of the Annex or its obligations under the Data Protection Laws;
3. the Supplier fails to comply with a binding decision of a competent court or supervisory authority/ies regarding its obligations pursuant to the Annex or Data Protection Laws;
4. the Supplier becomes aware of any circumstance or change in the Data Protection Laws or other laws applicable thereto that are likely to have a substantial adverse effect on the Supplier’s ability to meet obligations under this Annex.

(d) The Supplier shall be entitled to terminate the Services Agreement insofar as it concerns processing of Marionnaud Personal Data under this Annex where, after having informed Marionnaud that its instructions infringe applicable legal requirements in accordance with Clause 4(c), Marionnaud insists on compliance with the instructions.

Clause 20: Deletion or Return of Personal Data

(a) In the event the processing of Marionnaud Personal Data is completed or the Agreement terminated, the Supplier shall immediately cease the processing of the Personal Data and, at the choice of Marionnaud, either:

(i) delete all Personal Data processed on behalf of Marionnaud and certify to Marionnaud that it has done so; or

(ii) return all Personal Data to Marionnaud at a location directed by Marionnaud and delete existing copies of such data.

(b) In execution of the above, the Supplier shall immediately delete all Marionnaud Personal Data in its possession in such a way as to render such data irrecoverable by any means (including, without limitation, deleting Marionnaud Personal Data from its databases and destroying all backup or archive copies thereof) and furnish Marionnaud with a certificate signed by a duly authorised director of the Supplier certifying that this has been done.

(c) In cases where the Supplier is prohibited by applicable laws from deleting Marionnaud Personal Data, the Supplier shall inform Marionnaud and Parties shall prepare a plan on when and how such Personal Data will be deleted.

(d) Until the Personal Data is returned or deleted, the Supplier shall continue to ensure compliance with this Annex and applicable Data Protection Laws.

Clause 21: Indemnity

The Supplier shall indemnify and keep Marionnaud indemnified against all costs, claims, losses, damages, liabilities and expenses (including legal expenses) arising out of, or in connection with, any breach of this Annex, including breaches caused by its employees, agents and/or Sub-Processors in accordance with the applicable Data Protection Laws.

## **Appendix I - List of Parties**

Data Controller(s):

1. Name: Marionnaud Lafayette SAS

Address: 115 rue Réaumur, 75002 Paris .

Contact person’s name, position and contact details: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Signature and accession date:

Data Processor(s):

1. Name: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Address: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Contact person’s name, position and contact details: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Signature and accession date: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

2.

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

## **Appendix II - Description of Processing**

Categories of data subjects whose personal data is processed (employees data, prospective employees data and/or customers data) :

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Categories of personal data processed (e.g. identification data (name, surname, username), contact details (telephone number, email address)):

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Sensitive data processed (e.g. health data, biometric data):

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

* In case of Sensitive Data processing, indicate applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures) :

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Nature of the processing (collection, recording, organization, storage, adaptation, modification, extraction, consultation, use, communication by transmission or dissemination or any other form of provision and/or combination). . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Purpose(s) for which Personal Data is processed on behalf of the Data Controller (e.g. to ensure payroll management, to conduct a satisfaction survey). . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Duration of the processing. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

For processing carried out by Sub-Processors, also specify subject matter, nature and duration of the processing. please complete Annex IV below.

## **Appendix III - Appropriate Technical and Organisational Measures**

**General Requirements**

1. The Supplier shall not carry out any act or make any omission which has, or could reasonably be expected to have, an adverse impact on Marionnaud systems or Marionnaud Personal Data.
2. In assessing the appropriate level of security, the Supplier shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.
3. If the processing involves Sensitive Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences, the Supplier shall apply specific restrictions and/or additional safeguards.

**SECURITY STANDARDS**

***[Requirements for cloud services: e.g. hosting providers, SaaS tools]***

1. The Supplier is registered as part of the Cloud Security Alliance Security, Trust and Assurance Registry (STAR) Program – with the minimum level of registration as LEVEL ONE: CSA STAR Self-Assessment.

***[OR alternative wording in the case of a) cloud services provider not being CSA star registered or b) the supplier does provide IT services, but they are not in the cloud]***

1. The Supplier shall be ISO 27001 certified. The scope of ISO 27001 certification shall include all the sites and teams which are delivering services to Marionnaud.
2. The Supplier shall provide Marionnaud with the results of the Supplier’s latest ISO 27001 certification audit and its Statement of Applicability promptly upon request by Marionnaud. The results must include any findings, observations and non-conformities, together with associated mitigation plans and regular status updates for the mitigation work.

***[OR alternative wording in the case of not being ISO certified]***

1. The Supplier shall, and shall procure that the Supplier’s sub-contractors and each Supplier Personnel shall, ensure that their security management in connection with the Services, at a minimum, is implemented in accordance with the “Controls” and “Implementation Guidance” as defined and set out in ISO 27001, including clearly defined security responsibilities, processes for risk management, access control, authorisation and administration, security design and configuration management, audit and assurance.
2. The Supplier shall comply with security best practice as set out in ISO 27001 and ISO 27002 (or any standards replacing and or updating the same), and Marionnaud IT security team and its delegates may review and confirm the ongoing existence and compliance and/ or review, assess and confirm the adequacy of security management of the Supplier and/ or any sub-contractor of the Supplier in relation to the provision of the Services*.*

**SECURITY ORGANISATION**

1. The Supplier shall have an information security function, which has responsibility for ensuring good practice in relation to information security across the Supplier’s organisation and in relation to the provision of the Services, including the publication of information security policies.
2. The head of the Supplier's information security function shall be responsible for information security across the Supplier’s organisation.
3. The Supplier shall ensure that the Supplier's information security policies are at all times observed by the Supplier in the course of providing the Services.

**ACCESS MANAGEMENT**

1. Where the Supplier provides services connected directly to the Marionnaud systems, the Supplier must validate the identity of all the Supplier Personnel with access to Marionnaud systems. The Supplier must notify Marionnaud upon request of the names of the Supplier Personnel and the required and actual levels of access to Marionnaud information.
2. The Supplier will ensure that the obligations in Clause 12 above are supported by internal audit trails and alert monitoring to enable proactive identification of breaches and enable investigations, and there are clear real time audit reports and user activity audit trails to keep track of who is looking at what, when and what changes have been made.

**PHYSICAL SECURITY**

1. The Supplier is responsible for protecting Marionnaud Personal Data from harm through unauthorised physical access and/ or damage. This includes physical access controls such as protecting buildings against unauthorised access (e.g. by using locks, bolts or equivalent measures on vulnerable doors and windows), restricting physical access to critical areas to authorised staff only, supervising external parties when they are granted access and protecting communication links and data storage media.

**SECURITY AND PRIVACY REVIEW**

1. The Supplier shall permit Marionnaud personnel, authorised representatives and any party to whom Marionnaud is legally obliged to provide access or audit rights, to review and assess the Supplier’s compliance with the obligations set out in the Annex and this Appendix 2 of the Annex (the “**Security and Privacy Review**”).
2. The reviewers noted in Clause 15 above shall be entitled to, in respect of the Supplier, and /or its sub-contractors, access the premises controlled by them, extract any Marionnaud Personal Data held on their IT systems, inspect their security risk management controls and procedures, and interview the Supplier Personnel in order to assess compliance with the obligations set out in the Annex and this Appendix 2 of the Annex.
3. Subject to Clause 18 below, Marionnaud shall be entitled to conduct a review in accordance with this Appendix 2 of the Annex no more than once per annum.
4. The Supplier and/ or its sub-contractors (as applicable) shall remediate any failures identified by the Security and Privacy Review as directed by Marionnaud, including developing a comprehensive remediation solution for identified gaps and obtain Marionnaud approval for implementation. The cost of remediation shall be borne by the Supplier and/ or its sub-contractors (as applicable).

**EXPLANATORY NOTE:**

The technical and organisational measures need to be described concretely and not in a generic manner.

Description of the technical and organisational security measures implemented by the Supplier (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons :

………………………………………………………………………………………………………………………………………………………………………………………………………………………....……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………....

Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

For transfers to Supplier and/or its Sub-Processors, also describe the specific technical and organisational measures to be taken by the Supplier and/or its Sub-Processors to be able to provide assistance to the Controller.

Description of the specific technical and organisational measures to be taken by the Supplier or its Sub-Processors to be able to provide assistance to the controller :

………………………………………………………………………………………………………………………………………………………………………………………………………………………....……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………....

## **Appendix IV - List of Sub-Processors**

**List of Approved Sub-Processors**

The Data Controller has authorised the use of the following Sub-Processors:

1. Name: ....................................................................................................................................................

Address: .....................................................................................................................................................

Contact person’s name, position and contact details : ..........................................................................

............................................................................

Description of the processing (including a clear delimitation of responsibilities in case several Sub-Processors are authorised): ........................................................................................................................

..............................

Location from the services will be provided by the Sub-Processor: ..............................

In the case of an International Data Transfer, specify the corresponding International data transfer mechanism (e.g. adequacy decision of the European Commission, standard contractual clauses): .........................................................................................................

2. . .