AB Cube – 83 Avenue Philippe Auguste
75011 Paris, France
Tel : +33 1 88 40 17 80 99– www.ab-cube.com

GENERAL TERMS AND CONDITIONS (T&C) FOR AB CUBE SOFTWARE PRODUCTS AND SERVICES

These General Terms and Conditions governs the Customer's and End User's use of the Software Package and are incorporated by reference into the General Terms for the subscription to the Software Package between Customer and EXTEDO.

AB Cube, a limited liability company with a share capital of 20,000 EUR, with its registered office located at 83 Avenue Philippe Auguste, 75011 Paris, France, represented by Mr Matthieu DORESSE, in the legal capacity as CEO (the "SERVICE PROVIDER"). AB CUBE is a company specialized in supplying vigilance software with the databases SafetyEasy PV, SafetyEasy MD, SafetyEasy MI, CosmEthics and related modules in its catalogue of products.

These General Terms and Conditions applies to you or to the company or legal entity you represent ("You" or the "END USER") when using or accessing the databases SafetyEasy PV; SafetyEasy MD, SafetyEasy MI, CosmEthics and its related services (the "Software Package").

Both, You and the Service Provider will be referred hereinafter as "the Parties".

These T&C are intended to define the terms and conditions under which the END USER entrusts to the SERVICE PROVIDER the performance of the services defined below.

ARTICLE 1: SUBJECT OF THE T&C

This T&C is intended to define the terms and conditions under which the END USER entrusts to the SERVICE PROVIDER the performance of the services defined below.

ARTICLE 1 Bis: DEFINITIONS

“personal data” means any information relating to an identified or identifiable natural person (hereafter referred to as “data subject”); 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.

“GDPR” means, as regards its application to the French territory only, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural person with regard to the processing of personal data and on the free movement of such data (“General Data Protection Regulation” or “GDPR”) and the French national rules adopted on the basis of the provisions of this Regulation.

“Software Package” means the software, database and additional services provided by the SERVICE PROVIDER to the END USER. It includes the following databases:

- SafetyEasy PV™ (pharmacovigilance database)
- SafetyEasy MD™ (medical device vigilance database)
- CosmEthics™ (cosmetovigilance database)
- SafetyEasy MI™ (medical information database)
  - iTAP module
- Gateway between a SafetyEasy database and an Agency or AB CUBE

“Use and Access Rights” means the limited rights granted by the SERVICE PROVIDER to You as the END USER upon acceptance of the present Terms and Conditions.

The “Reseller” means EXTEDO GmbH, as the Service Provider’s partner that provides subscription services to the Software Package.

ARTICLE 2: DEFINITION OF THE SERVICES

The SERVICE PROVIDER undertakes to perform on behalf of the END USER the services (hereafter, the “Services”) as defined below:

2.1 – Providing Access to the Software Package and Documentation

The SERVICE PROVIDER undertakes to allow access to its **Software Package** database for all the entities of the END USER and for an unlimited number of users. The Parties agree that "users" shall be understood as, the employees of any entity of the END USER, the distributors of products bearing the brands of the END USER worldwide or the vigilance service providers of the END USER. The database will be delivered as a SaaS with web access. It is understood that the Software Package is strictly a single tenancy database: it can only be used to work on clinical or post marketing Individual Case Safety Reports coming from the entities or affiliates of the END USER.

Specific provision for CRO. With regard to the CRO model, the Parties agree that "users" shall be understood as: (a) the employees of any entity of the End User or (b) the clients of the End User, for whom the End User provides safety cases processing services using the Software Package. The database(s) will be delivered as a SaaS (Software as a Service) with web access. It is understood that the Software Package is strictly a single tenancy database: each database can be used to work on clinical or post marketing Individual Case Safety Reports linked to the activities of one company (or sponsor) and its affiliates only. The End User should use different Software Package databases for each of their clients.

The SERVICE PROVIDER notes that the minimum required configuration for the operation of the **Software Package** database is as follows:

- **Operating system:** Windows 98 or higher; or Mac OS X
- **Browsers:** Chrome all versions; Firefox all versions; Internet Explorer V ≥ 10; Safari: all versions;
  Opera: all versions
- **Internet connection:** minimum rate of 128 KB/s.
- Microsoft Excel, Word 2003 (or higher) or Open Office Calc (2.1 or higher).
- Acrobat Reader 6.0. or higher.

The **Software Package** operates using the MedDRA dictionary. As per the MSSO rules, the END USER declares that they have subscribed and will keep a license for use of the MedDRA dictionary as long as the **Software Package** software is used.

2.2 – Hosting Services for the Software Package Database

The hosting of the **Software Package** database is provided by a third party who acts as a subcontractor of the SERVICE PROVIDER. This third party is subject to the exclusive responsibility of the SERVICE PROVIDER who guarantees the security and integrity of the data hosted by this third party. See Appendix 1,2 & 3.

2.3 – Support Services for the Software Package Database

The SERVICE PROVIDER will provide support service for the Software Package database. The language used for the exchanges between the SERVICE PROVIDER and the END USER may be either English or French, at the END USER's discretion.

2.4 - Maintenance Services for the Software Package

As an exception, the SERVICE PROVIDER's maintenance operations may cause temporary access difficulties and short-term interruptions, of less than 1 hour. The SERVICE PROVIDER shall limit as much as possible the extent of the maintenance operations. Save in urgent and unforeseeable circumstances, the SERVICE PROVIDER will inform the END USER of the occurrence of these operations no later than 24 hours in advance so that the END USER can take any necessary steps. The END USER declares that he has been informed of this and agrees that the site may be temporarily interrupted in case of maintenance operations.

In cases where the maintenance operations cause interruptions exceeding one hour, the SERVICE PROVIDER shall immediately inform the END USER.

However, the SERVICE PROVIDER shall not provide maintenance services in the following cases:

- In the event of a change of equipment by the END USER which causes a modification of the minimum required configuration described in Article 2.1 of this T&C, without the consent of the SERVICE PROVIDER. The END USER may consult the SERVICE PROVIDER concerning the (physical and application) equipment that he wishes to acquire and check its compatibility with the software.
- In the event of any non-payment of fees owed to the SERVICE PROVIDER by the END USER for maintenance services.

2.5 – Updating Services for the Software Package Database

The SERVICE PROVIDER is brought to develop new functionalities or new regulatory tools for the **Software Package** database due to changes in the applicable legislation, in particular the European regulations concerning the **Pharmaceutical products** and the European regulations concerning the protection of personal data. In such cases, the SERVICE PROVIDER shall provide the END USER with programs and procedures adapted to the new version of the software, so that the functionalities of the software provided to the END USER are not affected.
Accessing the Service, the END USER agrees to accept all corrective and evolutionary maintenance offered by the SERVICE PROVIDER at the contracted rate.

However, the SERVICE PROVIDER is not required to ensure the adaptation and development of the **Software Package** database if the END USER decides to create a new environment for which the software package was not planned. Similarly, a significant change of the configuration of the (physical and application) equipment by the END USER cannot involve the SERVICE PROVIDER to undertake an adaptation of the software package within the framework of this T&C.

2.6 – Conformity of the Software Package Database

The SERVICE PROVIDER guarantees the conformity of the **Software Package** database with the functional and technical definitions appearing in the "Functional Specifications" provided by the SERVICE PROVIDER (Last version available through the software).

This guarantee of conformity is granted, provided that the END USER observes the utilisation procedures specified in such "Functional Specifications.

The SERVICE PROVIDER will provide the elements of validation file (IQ OQ PQ) to the END USER through the Document Management System. The SERVICE PROVIDER will also provide adequate validation documentation following GAMP 5 throughout the life of the product for each release of new versions of the software. It is the responsibility of the END USER to verify the validation of the software in their environment and maintain the validation throughout the software life, thanks to the validation's documents provided by the SERVICE PROVIDER.

The SERVICE PROVIDER guarantees the conformity of **Software Package** database with FDA 21 CFR PART 11 and EU GMP Annex 11. The SERVICE PROVIDER's validation process is described by Standard Operating Procedure: SOP Validation Master Plan.

The SERVICE PROVIDER does not guarantee the adaptation of the **Software Package** database to the specific requirements of the END USER, to the extent that the latter has verified in advance the appropriateness of its requirements to the functions and specifications set out in the documentation.

The END USER is responsible for:

- The implementation of operating procedures which ensure the correct use of the **Software Package** database.
- The results obtained and any direct or indirect consequences which may result from the use thereof.

The SERVICE PROVIDER confirms that he is fully informed of the applicable regulations for the protection of personal data, particularly the provisions of the GDPR, and that he undertakes to strictly comply with the provisions of the said regulations.

By accepting this T&C, the SERVICE PROVIDER undertakes to comply unconditionally and within the shortest time with any instruction by the END USER connected with the observance of applicable regulations concerning the protection of personal data or caused by an injunction by a concerned person or a supervisory authority. Any failure by the SERVICE PROVIDER to comply with such instruction from the END USER shall be considered to be a serious violation of the terms of the T&C and shall create a right for the END USER to terminate the T&C in advance, without notice or compensation. In addition, the SERVICE PROVIDER commits to indemnify or guarantee the END USER and to release the END USER from liability as a result of any complaints, actions, amicable procedures, arbitration or public or private court procedures and their consequences in terms of losses, costs or damages resulting from the SERVICE PROVIDER's failure to comply as soon as possible with the instructions of the END USER in connection with this Article.

ARTICLE 3: OBLIGATIONS OF THE PARTIES

3.1 – Obligations of the SERVICE PROVIDER

For the performance of the Services, the SERVICE PROVIDER acknowledges that with regard to the END USER he is held to an obligation of results for the Services which are measured by a service or time commitment indicator, and an obligation of means for the other Services.

The SERVICE PROVIDER is fully advised that the Services for which he is responsible for under the present T&C, requires on its part a general duty to provide assistance, information, advice and warnings in an ongoing concern for the correct performance of such Services.

In this connection, the SERVICE PROVIDER commits in particular:

- to collaborate in analysing the END USER's requirements, by requesting, if necessary, any information and/or documents needed for full understanding of the objectives, requirements and specificities of the END USER;
- to advise the END USER in all phases of the Project and in particular to make any suggestion which may improve the realization of the Project and the quality of the products delivered;
- to inform the END USER of any difficulty encountered in organizing or monitoring the tasks carried out by the END USER's staff or by any third party participating in the Services;
- to alert the END USER of any event of which he is aware and that may affect the correct performance of the Services (costs, schedule and timeframes, scope), including if this event is attributable to the END USER or if it is outside of the scope of the Services, but may have an impact on them;
- to advise the END USER on any choice or request made by the END USER of which he may be aware and which may affect the objectives of the Services or have an effect on the conditions for their performance;
- to advise and formally warn the END USER if the END USER issues additional or new requests during the performance of this T&C, particularly in terms of the impact on the timeframes and on the technical and financial conditions of the T&C;
- to observe the timeframes and the costs allocated for the Services, and the contractual commitments;
- to possess and maintain the skills necessary for the performance of the Services.

3.2 – Obligations of the END USER

The END USER is not allowed to make any copy of the **Software Package** database or any reproduction or adaption thereof, whether total or partial.

The END USER may not undertake either directly or indirectly the transmission, transfer or any provision of the **Software Package** database, whether free of charge or for payment, to any third party other than the companies listed in Article 2.1.

In order to allow the SERVICE PROVIDER to correctly perform the Services, the END USER must provide active and diligent collaboration in the course of this T&C and in this connection. The END USER commits:

- to ensure the effective participation of its necessary staff each time that the correct performance of the Services requires it;
- to freely provide the SERVICE PROVIDER with all the data necessary for the correct performance of the Services;
- to keep the SERVICE PROVIDER informed of any change which affects its decision-making structure or its organisation and which has an impact on the performance or the scope of the Services.

3.3 – Joint Undertaking of the Parties

All Services shall be carried out in T&C with a method of collaboration which brings together the END USER's team with the SERVICE PROVIDER's team.

To this end, both parties undertake to maintain permanent dialogue and collaboration between them, as well as the END USER with the SERVICE PROVIDER, in order to allow the correct performance of this T&C.

The END USER reserves the right to audit the SERVICE PROVIDER, within a limit of once a year, in order to verify the application of the provisions provided for by this T&C. The END USER will notify the SERVICE PROVIDER at least 45 days before the audit realization.

ARTICLE 4: DURATION

This T&C become effective as from the date of the subscription and acceptance through EXTEDO (The "Reseller") Terms of Use. The duration of the present T&C shall be effective for the period set up in the order request through the Reseller subscription process. Unless expressly terminated this T&C shall be automatically renewed for successive periods of 1 year accordingly to the renewal of the subscription to the Software Package

ARTICLE 5: PRICES WITHOUT TAX / PAYMENT TERMS

5.1– Payment

The price for the Software Package database and the terms of payment will be invoiced by and paid to the Reseller.

5.2– Annual pricing revision:

The SERVICE PROVIDER is a member of the French Syntec Federation. In accordance with the Syntec Federation policy, the SERVICE PROVIDER will enforce an annual pricing revision based on the Syntec index, which represents the evolution of the labour costs for the branch. This will be reflected on the price that the Reseller will invoice the End User.

ARTICLE 6: PENALTIES FOR DELAY

The SERVICE PROVIDER undertakes to observe the timeframes for response and resolution as indicated in the Customer Support Guidelines.

In the event of a failure to observe these timeframes for response and/or resolution, the SERVICE PROVIDER shall be automatically subject to pay the cost of the delay in the sum of 1% of the monthly hosting cost per day of delay and each day commenced shall be due.
Delays connected with external factors not directly attributable to the SERVICE PROVIDER shall not be subject to penalties.

6.1 Penalty CONTINGENCY

The applicability of penalties for the non-respect of deadlines regarding the installation, training and data migration are contingent on the acceptance of the present T&C.

ARTICLE 7: LIABILITY – INSURANCE

7.1– Responsibility of the SERVICE PROVIDER

The SERVICE PROVIDER is responsible for damages suffered by the END USER as a result of possible failures or negligence in the performance of the Services.

The SERVICE PROVIDER is also responsible for the actions of its employees, subcontractors and possible agents acting in the performance of the T&C.

Any such liabilities referred to above shall be capped at the value of the insurance policy in place at the relevant time.

7.2– Responsibility of the END USER

The END USER shall ensure the implementation of operating procedures which ensure the correct use of the software package.

The END USER shall be responsible for the results obtained from using the Software Package database and any direct or indirect consequences which may result from the use thereof.

7.3– Insurance

The SERVICE PROVIDER is required to insure with a reputably solvent insurance company for its civil, professional and operational liability in order to cover the monetary consequences for the END USER of bodily injury, property and immaterial damages which the END USER may suffer as a result of any event which may be attributable to the SERVICE PROVIDER or its employees in the course of performing the Services subject to this T&C.

This includes in particular damages caused to equipment, software, the software package, data files or other documents provided or used by the SERVICE PROVIDER in connection with the Services.

Upon the END USER’s first request, the SERVICE PROVIDER must transmit to it a certificate from the insurance company specifying the subject, the duration and the extent of the guarantee, the exclusions and the amount of the insured risk.

The SERVICE PROVIDER undertakes to maintain this insurance coverage in force throughout the entire duration of the T&C.

ARTICLE 8: TERMINATION

These T&C will remain in effect until the termination of the subscription with the Reseller. The End User may terminate the subscription by contacting the Reseller (EXTEDO). The Reseller will establish the conditions for termination on which the End User may cancel the Subscription to the Software Package.

ARTICLE 9: SUBCONTRACTING

If the SERVICE PROVIDER wishes to subcontract all or part of the Services, he commits to inform the END USER of this and proceed only after receiving the END USER’s prior written consent.

If the use of subcontracting is authorised, the SERVICE PROVIDER commits to comply with any normative, legal or regulatory provision relating thereto (such as, in particular, and without this list being exhaustive, as concerns labour law, normative rules such as BPF ISO 22716, and the submission of the mandatory documents by each subcontractor as defined by the texts in force as of the date of signing this T&C).

The SERVICE PROVIDER undertakes to ensure that the terms for the performance of the Services are observed and shall consequently be responsible for the subcontracted Services with regard to the END USER and shall retain final responsibility for the performance of its mission from a monetary and technical point of view.

ARTICLE 10: INTELLECTUAL PROPERTY

10.1– Rights of the END USER

The SERVICE PROVIDER acknowledges that all the documents provided by the END USER in order to perform the requested Service are and shall remain the exclusive property of the END USER.

The SERVICE PROVIDER shall, for its part, refrain from any personal use of the database and files, without the express written permission of the END USER. The SERVICE PROVIDER commits to observe absolute confidentiality with regard to all of the information and activities related to the END USER in the context of this T&C.

The SERVICE PROVIDER regularly files with the APP (the Agency for Protection of Programmes") the sources of the software package and in accordance with the provisions of the APP, in the case of the bankruptcy of the SERVICE PROVIDER (bankruptcy and non-acquisition by a third party), the END USER shall have the possibility to access the sources at APP, 119 rue de Flandres 75019 PARIS.

Registration No. IDDN.FR.001.430013.000.S.P.2012.000.30000.

The SERVICE PROVIDER declares that all of the data recorded by means of the **Software Package** database are the exclusive property of the END USER.

Upon the termination of the T&C, the SERVICE PROVIDER will provide the END USER with all of the data owned by the END USER in a format that it or any new service provider selected by the END USER can use (XML format + DUMP of the tables). The SERVICE PROVIDER will provide this data at the date determined by the END USER, provided that the END USER gives notification to the SERVICE PROVIDER 2 weeks in advance. The SERVICE PROVIDER shall not charge any fee to the END USER for this service. The SERVICE PROVIDER also commits to provide the END USER or the new service provider selected by the END USER with any necessary assistance for the handover, without interruption of the services for the END USER or the new service provider.

All of the documents and materials relating to these Services must be returned to the END USER upon its request without the SERVICE PROVIDER retaining a copy and the SERVICE PROVIDER shall refrain from re-using all or part of these in any form whatsoever.

10.2– Rights of the SERVICE PROVIDER

The SERVICE PROVIDER is the sole owner of the intellectual and industrial property rights to the **Software Package** database.

The SERVICE PROVIDER declares that the software package subject to this T&C is its property or that it holds a legal right to market such software package.

The END USER commits not to harm the rights of the SERVICE PROVIDER directly or indirectly or by the intermediary of a third party with which it is associated.

In the event of an action for infringement with regard to the software package brought by a third party against the END USER, the END USER shall immediately inform the SERVICE PROVIDER.

The END USER commits to take the necessary steps to ensure the secrecy, confidentiality and observance of the ownership of the software package with regard to its personnel or any external person who may have access to the software package.

ARTICLE 11: CONFIDENTIALITY

The END USER and the SERVICE PROVIDER agree that the information that they have received to date or will receive in the future from the other Party and which is directly or indirectly related to the areas governed by this T&C (1), shall remain the exclusive property of the Party which is the source, (2) shall be scrupulously kept confidential by both Parties, (3) shall not be used other than in connection with and throughout the duration of this T&C by the Party that is not the source, whereas the Party that is the source may freely use this information whether during the performance of this T&C or after its expiration or termination for any reason whatsoever and (4) shall not be disclosed to third parties by the Party which is not the source without having obtained the prior written consent of the Party that is the source. The information which is already entirely in the public domain, received from third parties which are not required to keep it confidential or that one of the Parties is required to disclose in application of legal or regulatory provisions shall not be covered by this Article.

Each Party shall ensure that its employees and/or possible subcontractors shall comply with this confidentiality obligation. With regard to its staff, each Party shall take all necessary measures to ensure the secrecy and the confidentiality of all of the information addressed by this Article.

The provisions of this Article shall remain in force for a period of five (5) years after the termination of this T&C.

ARTICLE 12: PROTECTION OF PERSONAL DATA

In performing this T&C, the SERVICE PROVIDER may be required to process personal data on behalf of and on the instructions from its END USER.

In this context, the END USER is acting as the controller and the SERVICE PROVIDER as the processor within the meaning of the rules applicable in France and in the European Union regarding the protection of personal data, except for the CRO business model, in which case the END USER is a processor and the SERVICE PROVIDER is a sub processor. The SERVICE PROVIDER is therefore subject to the obligations of Article 28 of the General Data Protection Regulation[1] (hereafter, “GDPR”).

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural person with regard to the processing of personal data and on the free movement of such data, and

As such, the SERVICE PROVIDER undertakes to process the personal data entrusted by the END USER in accordance with the END USER's written instructions and the provisions set out in Appendix 1 "Protection of Personal Data," with which the SERVICE PROVIDER expressly represents that it is able to comply.

ARTICLE 13: STAFF OF THE SERVICE PROVIDER

13.1– Obligations of the SERVICE PROVIDER as an Employer

The staff of the SERVICE PROVIDER assigned to manage this T&C shall remain, in all circumstances, under the full supervision and discipline of the SERVICE PROVIDER.

If applicable, the staff of the SERVICE PROVIDER must comply with the instructions for working, health and safety that are in force at the END USER's site, as well as the END USER's internal regulations. The presence of the SERVICE PROVIDER's staff on the END USER's site shall not in any event constitute a loan of labour.

The SERVICE PROVIDER declares that it has met the legal and regulatory requirements concerning:

- concealed labour;
- and foreign labour employment.

The SERVICE PROVIDER shall bear all of the penalties and more generally any payment which the END USER may be assessed or forced to pay as a result of the SERVICE PROVIDER's violation of the regulations in terms of labour or tax law.

13.2– Obligation to Maintain Skills

The SERVICE PROVIDER commits to provide the human resources and skills necessary to ensure strict compliance with the Schedule.

The SERVICE PROVIDER commits to assign staff to the performance of the T&C who possess the professional skills and experience necessary for the correct performance of the Services.

The SERVICE PROVIDER commits to maintain the stability of the principal staff assigned to performing the Services throughout the entire duration of the T&C, except in the case of force majeure.
The SERVICE PROVIDER commits to ensure the continuity of performance of the Services, in accordance with the timeframes provided for by the T&C, particularly in the case of illness or resignation of an employee of the SERVICE PROVIDER or for any other reason.

repealing Directive 95/46/EC (General Data Protection Regulation). The GDPR applies from 25 May 2018 onwards; before 25 May 2018 the Directive 95/46/EC applies.

ARTICLE 14: INDEPENDENCE OF THE PARTIES

Both Parties agree to act as independent parties in connection with the T&C. Consequently, the T&C may not in any event be considered to be a document constituting a legal entity of any sort. The Parties declare that any form of "*affectio societatis*" is formally excluded.

In this regard, the T&C may not in any event create a connection of subordination between the personnel of the SERVICE PROVIDER and the END USER which is characterised by a salaried relationship between the persons assigned by the SERVICE PROVIDER to perform the orders subject to the T&C and the END USER.

The members of the SERVICE PROVIDER's personnel are solely subject to the decisions of the SERVICE PROVIDER in application of their employment T&Cs. They may only receive direct instruction from the SERVICE PROVIDER, which shall be responsible for their remuneration as well as all of their costs.

ARTICLE 15: MISCELLANEOUS PROVISIONS

15.1– Non-Exclusivity

This T&C does not contain any commitment of exclusivity or guaranteed minimum turnover by the END USER with regard to the SERVICE PROVIDER.
The SERVICE PROVIDER acknowledges that it is its entire responsibility to seek for enlarging its END USER lists and that it may not therefore bring any complaint against the END USER for allowing a situation of economic dependency to be established as a result of the application of this T&C.

The SERVICE PROVIDER acknowledges that throughout the duration of this T&C, it shall be solely responsible in the event of insufficient diversification of its END USERs, particularly with regard to its own suppliers and possible subcontractors.

15.2– Intuitu Personae

The T&C is concluded by the END USER in consideration of the person and the specific skills of the SERVICE PROVIDER. The SERVICE PROVIDER is not authorised to transfer this T&C whether by assignment, transfer of on-going business, merger or other means, without the prior written consent of the END USER.

ARTICLE 16: APPLICABLE LAW AND JURISDICTION

This T&C is subject to French law.
Any modification of the T&C may only be taken into consideration after signature of an amendment by the Parties.
Any dispute between the Parties concerning the interpretation, performance or termination of this T&C which has not been settled amicably shall be subject to the jurisdiction of the Commercial Court of Paris.

ARTICLE 17: LIST OF APPENDICES

APPENDIX 1: Protection of Personal Data

APPENDIX 2: List of the SERVICE PROVIDER's sub-processors

APPENDIX 3: Hosting of the SOFTWARE PACKAGE

APPENDIX 1: Protection of Personal Data

1. Preamble

For the purposes of the T&C for the Provision of Services (hereafter, the "T&C"), the SERVICE PROVIDER may access personal data of patients and healthcare professionals when performing support, maintenance and hosting services, which are processing of personal data within the meaning of the General Data Protection Regulation (hereafter, "GDPR").

The SERVICE PROVIDER acknowledges that all of the personal data it may again access in that context are strictly confidential. Therefore, the SERVICE PROVIDER acknowledges that all data processed in connection with the performance of the T&C:

- are subject to the rules applicable in France and in the European Union regarding the protection of personal data (hereafter, "personal data protection rules") including, without limitation:
  - the French Data Protection Act[2];
  - the General Data Protection Regulation[3];
  - where applicable, texts adopted within the European Union and local laws that may apply to the personal data processed within the framework of the T&C;
  - texts and decisions issued by supervisory authorities, in particular the French data protection authority (Commission nationale de l'informatique et des libertés, hereafter referred to as "Cnil");
  - where applicable, texts and recommendations adopted by the Article 29 Data Protection Working Party or any organisation or authority in the field of personal data protection;

- concern privacy and professional secrecy.

The SERVICE PROVIDER undertakes to implement all necessary procedures to ensure their confidentiality and utmost security.

2. Purpose

This Appendix forms an integral part of the T&C entered between the SERVICE PROVIDER (as the processor) and the END USER (as the controller).

For the purposes of this Appendix the roles are set out on the basis of END USER (Controller) and SERVICE PROVIDER (as Processor), except for those END USERS with a CRO business model, where the roles may

[2] French Data Protection Act No.78-17 of 6 January 197, as amended and updated.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural person with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). The GDPR applies from 25 May 2018 onwards; before 25 May 2018 the Directive 95/46/EC applies.

encompass processor-subprocessor relationship: END USER as the processor and SERVICE PROVIDER as sub-processor.

This Appendix sets out the terms and conditions under which the SERVICE PROVIDER undertakes to:

- perform the data processing operations defined below on behalf of the END USER;
- adopt the appropriate technical and organisational measures to ensure an appropriate level of security of the personal data processed.

Regarding the processing of personal data, the SERVICE PROVIDER acknowledges and agrees that it may only act in accordance with the provisions hereof.

3. Description of the processing

The SERVICE PROVIDER is authorised to process personal data on behalf of the END USER for the purposes of the performance of the services covered by the T&C.

3.1. Subject-matter of the processing

The processing operations of personal data by the SERVICE PROVIDER are intended to perform the services provided for in the T&C.

3.2. Duration

The processing operations carried out by the SERVICE PROVIDER on behalf of the END USER are carried out for the duration of the services provided by the SERVICE PROVIDER for the END USER.

3.3. Nature and purpose of the processing

The processing operations consist of support, maintenance and hosting operations in relation to the personal data collected and/or provided by END USERS and their service providers when using the SOFTWARE SOLUTIONS covered by the T&C.

The purpose of those processing operations is to perform the support, maintenance and hosting services included in the SOFTWARE SOLUTIONS.

3.4. Type of personal data processed

The categories of personal data processed are those collected and/or provided by the END USER or its provider, users of the SOFTWARE SOLUTIONS. This includes, without limitation:

- data related to the identity and contacts details of the patients;
- data related to the identity and contacts details of health professionals;
- data related to the health of patients;
- data related to adverse effects of patients;
- data related to the identity of the ticketing tool users.

3.5. Categories of data subjects

The categories of data subjects are in particular those whose data are collected and/or provided by the END USER or its provider, i.e. data concerning patients and healthcare professionals as well as data of the software users when using ticketing.

4. Warranty

The SERVICE PROVIDER warrants the END USER the compliance with its statutory and regulatory obligations as a processor under the personal data protection rules and the compliance with its obligations under this Appendix.

The END USER warrants the SERVICE PROVIDER the compliance with its statutory and regulatory obligations as a controller, in particular under the personal data protection rules, and the compliance with its obligations under this Appendix.

5. Obligations of the processor

The SERVICE PROVIDER undertakes to take all necessary measures for compliance by itself and by its personnel with its obligations as listed below:

- not to process or consult the data for purposes other than the performance of the services it performs on behalf of the END USER hereunder;

- not to process or consult the data except within the framework of the documented instructions and authorisations received from its END USER, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by a mandatory rule resulting from EU or EU Member State law to which the SERVICE PROVIDER is subject. In such a case, the SERVICE PROVIDER shall inform the END USER of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

- take all measures referred in these T&C and Appendix to help prevent abusive, malicious or fraudulent use of the data;

- not to carry out statistical studies on the data or processing operations other than those requested by its END USER;

- immediately notify its END USER of any modifications or changes which may affect the processing of personal data, in particular to report any change relating to the administrative situation of the SERVICE PROVIDER to the END USER[4] by any appropriate means with acknowledgment of receipt;

[4] PGSSI-S, Rules for remote interventions on health information systems, rule [C3]

- immediately inform its END USER if, in the SERVICE PROVIDER's opinion, an instruction infringes the personal data protection rules.

The parties agree that an instruction shall be deemed to be given when the SERVICE PROVIDER acts within the framework of these Appendix and T&C.

The SERVICE PROVIDER undertakes to take all appropriate steps to ensure that natural persons acting under its authority and who have access to personal data do not process them except on instructions from the END USER, unless they are required to do so by a mandatory rule resulting from EU or EU Member State law applicable to the processing.

The SERVICE PROVIDER shall ensure that persons authorised to process the personal data have committed themselves to confidentiality.

The SERVICE PROVIDER acknowledges and agrees that it shall not process the data to which it may have access except in a manner consistent with these Appendix and T&C.

The SERVICE PROVIDER will provide the controller with the name and contact details of its Data Protection Officer[5].

6. Security

6.1. Main principles

In accordance with the personal data protection rules, the SERVICE PROVIDER undertakes to take all useful precautions referred to in this T&C, with regard to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their distortion, alteration, damage, accidental or unlawful destruction, loss, disclosure and/or access by third parties not previously authorised.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the SERVICE PROVIDER shall implement the appropriate technical and organisational measures referred to in this T&C to protect personal data and ensure a level of security appropriate to the risk.

6.2. Specific security measures

6.2.1. Specific security measures for all processing of the SERVICE PROVIDER

The means implemented by the SERVICE PROVIDER to ensure the security and confidentiality of the data are in accordance with the state of the art and the regulations in force.

In particular, the SERVICE PROVIDER undertakes to implement the following measures:

- encrypt personal data backups;

[5] The SERVICE PROVIDER is required to designate a DPO pursuant to Article 37 of the GDPR

- inform and raise awareness among its staff, including the signature by each person acting on behalf of the SERVICE PROVIDER of an individual confidentiality T&C annexed to his/her employment contract[6];

- access personal data by means of authentications[7] consistent with the recommendations issued by the Cnil[8];

- define authorisation profiles, remove obsolete access permissions and allow access to tools and administration interface only to qualified individuals[9];

- implement automatic traceability systems (logs, audits for regularly assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing)[10];

- define a security policy appropriate to the risks of the processing and including the security objectives as well as the physical, logical and organisational security measures to fulfil them[11];

- have the ability to restore the availability of and access to personal data in a timely manner as provided for in the T&C in the event of a physical or technical incident, in particular by regularly making backups;

The SERVICE PROVIDER undertakes to maintain those measures throughout the performance of the T&C and failing this, to inform the END USER.

In any event, if the measures used to ensure the security and confidentiality of the data are changed, the SERVICE PROVIDER undertakes to replace them by measures of superior performance. No change can lead to a reduction in the level of security.

6.2.2. Specific security measures for hosting health data

[6] PGSSI-S, Rules for remote interventions on health information systems, rule [C6]
[7] Authentication must at least comply with level 1 of the PGSSI-S's reference specification for the authentication of healthcare actors [private authentication: individual identifier/password with specific constraints particularly in terms of construction, storage and renewal].
[8] Cnil, Deliberation No. 2017-012 of 19-1-2017 adopting a recommendation on passwords, as amended
[9] Cnil, Guide de sécurité (CNIL's Guide "Security of Personal Data"), 2017.
[10] Cnil, Guide de sécurité (CNIL's Guide "Security of Personal Data"), 2017
[11] Cnil, Guide de sécurité (CNIL's Guide "Security of Personal Data"), 2017

The means implemented by the SERVICE PROVIDER to ensure the security and confidentiality of the data are in accordance with the state of the art[12] and include the hosting of data outsourced to an approved or certified hosting provider according to Decree No. 2018-137 of 26 February 2018 relating to the hosting of personal health data, as authorised by the END USER in accordance with article "Sub-processing" of this Appendix.

In compliance with the regulations on the hosting of personal health data, the contract between the SERVICE PROVIDER and the hosting provider, is available at all time on our Document Management System[13].

6.2.3. Specific security measures for remote interventions

Where the SERVICE PROVIDER processes the processing of data remotely, it complies with the applicable rules, regarding processing, set out in the Global Information Security Policy for the healthcare sector (hereafter "PGSSI-S") published by the Shared Healthcare Information Systems Agency (Agence des Systèmes d'Information Partagés de Santé)[14].

In addition to the measures referred to in paragraph "Specific security measures for all processing of the SERVICE PROVIDER" (6.2.1), the SERVICE PROVIDER implements the following security measures:

- measures to restrict local access to intervention workstations to authorised persons only. At a minimum, raise the awareness of authorised persons of the need to secure logical access to intervention stations and the associated security means; [15]

- means and procedures in conformity with the rules of the art to fight against incidents that could affect the security of the SOFTWARE SOLUTIONS or the software data or the security of the intervention (security incidents in the human, organisational, technical or physical environment); [16]

- means and procedures in conformity with the rules of the art to fight against malicious code and the exploitation of known vulnerabilities of the IT or telecommunication means put in place by the SERVICE PROVIDER for the service (e.g. reporting vulnerabilities for joint decision-making); [17]

[12] Hosting health data certification referential

[13] In accordance with Article R.1111-11 of the Public Health Code , resulting from Decree No. 2018-137 of 26 February 2018 on the hosting of personal health data: "[...] II.- When the data controller or the patient mentioned in I of Article R. 1111-8-8 calls upon a provider who himself uses a certified hosting provider to host the data, the contract that binds the data controller or the patient with his provider shall include the clauses mentioned in I as they appear in the contract binding the provider and the certified hosting provider."

[14] PGSSI-S, Règles pour les interventions à distance sur les systèmes d'information de santé, December 2014, V1.0

[15] PGSSI-S, Rules for remote interventions on health information systems, rule [E2]

[16] PGSSI-S, Rules for remote interventions on health information systems, rule [E4]

[17] PGSSI-S, Rules for remote interventions on health information systems, rule [E5]

- means and procedures in conformity with the rules of the art to fight against malicious code in the SOFTWARE SOLUTIONS or in its update, and against the exploitation of known vulnerabilities in these elements; [18]

The SERVICE PROVIDER undertakes to establish a security insurance plan in conformity with the rules of the art, including the description of the security provisions that the SERVICE PROVIDER implements for its service, at least in relation to the following topics[19]:

- the identification of the contact person in charge of the security of the interventions at the SERVICE PROVIDER;
- the security criteria used in the designation of the persons in charge of the remote intervention, security commitment, information and awareness of these persons on the security of the service;
- the rules for protecting information relating to the SOFTWARE SOLUTIONS or to the intervention and held by the SERVICE PROVIDER (copy, distribution, storage, destruction, transmission);
- the designation of the processing sites, physical protection and access to the premises used, separation from other services;
- the general architecture of the platform used for remote intervention, the technical partitioning from other services, the security features activated in the platform;
- the logical access of the participants in the platform, identification and authentication, automatic standby and disconnection, separation of tasks, rights management, traceability of actions;
- the arrangements made to continue the processing activities following a major disaster;
- the assurance and control of the security of the intervention services provided.

The practical modalities for the proper implementation of the corrective and evolutionary maintenance must be brought to the attention of the data subjects. In this respect, the following organisational security provisions must be taken into account[20]:

- the updated list of the persons who can request a remote intervention must be communicated to the SERVICE PROVIDER to allow its personnel to check the validity of the intervention requests[21]:

[18] PGSSI-S, Rules for remote interventions on health information systems, rule [E7]
[19] PGSSI-S, Rules for remote interventions on health information systems, rule [A1]
[20] PGSSI-S, Rules for remote interventions on health information systems, rule [01]
[21] PGSSI-S, Rules for remote interventions on health information systems, rule [02]

- plan remote monitoring and maintenance interventions. Filtering of remote access to the equipment concerned should only allow access during the periods of time agreed with the beneficiaries of these interventions. An exception procedure may be provided for temporarily authorising access outside these periods of time in order to meet emergency intervention needs.·[22]

For each intervention a remote access point (or gateway) is set up to access the remote intervention equipment.[23]

The SERVICE PROVIDER undertakes, as far as possible, to comply with the following measures:

- the equipment is connected to this access point by an administration network implemented either via a dedicated network physically separate from the rest of the SOFTWARE SOLUTIONS, or via a DMZ or any other mechanism allowing logical isolation between the administration flows and the rest of the SOFTWARE SOLUTIONS. This logical isolation will preferably be done by means of a VPN;[24]

- the remote access point must be protected against logical attacks from networks and its bypass, in order to access the SOFTWARE SOLUTIONS, must not be possible in practice;[25]

- the access point must be subject to renewed security audits to verify its implementation and its resistance to intrusion attempts in the SOFTWARE SOLUTIONS; [26]

- exchanges between the intervention platform and the remote access point to the SOFTWARE SOLUTIONS must be protected by encryption and mutual authentication functions. [27]

In the event of prolonged absence of traffic in a session, monitoring mechanisms must automatically close any exchange session (live or on either side of the access point) established between the platform and an item of equipment subject to the intervention. The automatic disconnection time, to be agreed according to the characteristics of the remote intervention, must be as short as possible[28];

7. Data breach

[22] PGSSI-S, Rules for remote interventions on health information systems, rule [03]
[23] PGSSI-S, Rules for remote interventions on health information systems, rule [T1]
[24] PGSSI-S, Rules for remote interventions on health information systems, rule [T2]
[25] PGSSI-S, Rules for remote interventions on health information systems, rule [T3]
[26] PGSSI-S, Rules for remote interventions on health information systems, rule [T4]
[27] PGSSI-S, Rules for remote interventions on health information systems, rule [T5]
[28] PGSSI-S, Rules for remote interventions on health information systems, rule [T10]

The SERVICE PROVIDER must, without undue delay after having become aware of it, notify the END USER of any personal data breach, namely a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

This notification must be sent to the person designated by the END USER as the contact point, and where applicable, to the Data Protection Officer, by e-mail, and confirmed by registered letter with acknowledgment of receipt. It shall describe the nature and consequences of the personal data breach, the measures already taken or proposed to be taken to address the personal data breach, the people from whom more information can be obtained, and where possible the approximate number of data subjects likely to be affected by the breach, and where applicable, the contact details of the Data Protection Officer or another The SERVICE PROVIDER's contact point from whom additional information can be obtained. The contact details of DPOs are the following: dpo@ab-cube.com

In the case of a data breach, the SERVICE PROVIDER undertakes to carry out any useful investigations on the violation of the protection rules in order to remedy them as soon as possible and mitigate their impact on the data subjects. The SERVICE PROVIDER undertakes to inform the END USER of its investigations on a regular basis.

The SERVICE PROVIDER undertakes to actively collaborate with its END USER to ensure that it is able to meet its regulatory and contractual obligations. As the controller, the END USER is solely responsible for notifying such personal data breach to the CNIL and, where applicable, for communicating the breach to the data subjects.

8. Sub-processing

The END USER authorises the SERVICE PROVIDER to use one or more other processors (hereafter referred to as "sub-processor(s)"), within the meaning of the data protection regulations, to outsource all or part of the services, in particular the hosting of the SOFTWARE SOLUTIONS with the sub-processor(s) listed in the Appendix 2: "list of sub-processors".

The SERVICE PROVIDER, which is therefore granted general written authorisation to engage one or more sub-processors to perform the services subject to the T&C, agrees to:

- inform and sign with its sub-processor a written T&C that makes reference to the T&C and this Appendix and imposes on its sub-processor the same data protection obligations as set out in these Appendix and T&C;

- impose on its sub-processor all obligations necessary to ensure that the confidentiality, security and integrity of the data are respected and that the said data can neither be transferred or leased to a third party, whether free of charge or for consideration, nor used for purposes other than those defined in these Appendix and T&C;

- send to the END USER a copy of the contract with its sub-processor(s) and, failing that, a description of the essential elements of the contract, including the implementation of the obligations relating to personal data protection;

- inform the END USER of any intended changes concerning the addition or replacement of sub-processors, thereby giving the END USER the opportunity to object to such changes;

- make available to the END USER a list of the sub-processor(s) involved in the processing of personal data.[29]

The data processed under the T&C shall not be disclosed to third parties, including the sub-processors of the SERVICE PROVIDER, except in the cases provided for in these Appendix and T&C or those provided for by a legal or regulatory provision.

Where its sub-processors fail to fulfil their data protection obligations, the SERVICE PROVIDER shall remain fully liable to the END USER for the performance of those sub-processors' obligations.

9. Transborder data flows

In the unlikely event that a transfer of personal data is required to a third country, not belonging to the European Union, or to an international organisation, the SERVICE PROVIDER must obtain the prior written authorisation of the END USER.

If such authorisation is granted, the SERVICE PROVIDER undertakes to cooperate with its END USER to ensure:

- compliance with the procedures for complying with the personal data protection rules, for example in case an authorisation from the CNIL is required;

- where applicable, the conclusion of one or more T&Cs to regulate such transborder data flows. The SERVICE PROVIDER particularly undertakes, if needed, to sign such T&Cs with its END USER and/or to obtain the conclusion of such T&Cs from its sub-processors. To this end, the parties agree that the standard contractual clauses issued by the European Commission will be used to provide a framework to transborder data flows.

10. Maintenance of a record

As a processor, the SERVICE PROVIDER undertakes to maintain a record of all categories of processing activities carried out on behalf of the END USER acting as the controller, in accordance with the provisions

[29] See list below

of Article 30 of the GDPR. The SERVICE PROVIDER shall make the record available to the END USER on request.

11. Storage of data

At the end of the T&C, the SERVICE PROVIDER undertakes to archive all manual or computerized filing systems that store the information collected solely for the duration necessary for its commercial obligations and for evidence purposes.

Where applicable, at the END USER's request, the SERVICE PROVIDER undertakes to return all the personal data to the END USER or to any sub-processor designated by the END USER.

The SERVICE PROVIDER undertakes to provide the END USER with a certificate of personal data suppression on request at the end of the archiving period.

12. Verifications

At the request of its END USER, the SERVICE PROVIDER shall draw up a certificate or transmit all information necessary to demonstrate that the rules provided for in this Appendix, and the obligations under the personal data protection rules, have been complied with.

According to the pricing conditions previously established by the SERVICE PROVIDER, the END USER reserves the right to conduct any verifications which it would deem useful to verify compliance with the above-described obligations, including a security audit of the SERVICE PROVIDER or directly of a sub-processor[30].

The SERVICE PROVIDER undertakes to respond to the END USER's audit requests made either by the END USER or by a trusted third party appointed by the END USER, recognised as an independent auditor, having the necessary qualifications.

The SERVICE PROVIDER warrants its END USER that it will carry out audits every two years at its hosting provider and make the relevant audit report available to the END USER.

Audits are intended to analyse the SERVICE PROVIDER's compliance with its obligations under this Appendix, the T&C and the personal data protection rules. In particular, they ensure that the security and confidentiality measures in place cannot be circumvented without being detected and reported.

13. Cooperation

The SERVICE PROVIDER undertakes to cooperate with the END USER to ensure:

- where applicable, the management of requests related to the exercise of data subjects' rights;

[30] PGSSI-S, Rules for remote interventions on health information systems, rule [C8]

- the carrying out of any impact assessment that the END USER would decide to carry out in order to assess the risks of the processing to the rights and freedoms of natural persons and to identify the measures to be implemented to deal with these risks, and the consultation with the CNIL. This service will be subject to a specific quote by the SERVICE PROVIDER.

- more generally, the compliance with the obligations imposed on the END USER by the personal data protection rules, such as its obligation of security[31] or its obligation to notify the CNIL and to communicate a personal data breach to the data subjects.

In the event of an inspection by a competent authority, the parties undertake to cooperate with each other and with the supervisory authority.

Apart from the services covered by the T&C, where the inspection relates only to the processing operations implemented by the SERVICE PROVIDER as a controller, the SERVICE PROVIDER shall be responsible for the inspection.

Where the inspection carried out at the SERVICE PROVIDER relates to the processing operations carried out in the name and on behalf of the END USER, the SERVICE PROVIDER undertakes to inform the END USER immediately and not to make any commitment on its behalf.

In the event of an inspection by a competent authority at the END USER relating in particular to the services provided by the SERVICE PROVIDER, the SERVICE PROVIDER undertakes to cooperate with the END USER and to provide it with any information which the latter may require or which would be necessary.

[31] GDPR, Art. 28(3)(f)

APPENDIX 2: List of the SERVICE PROVIDER's sub-processors

1. Hosting of health data

Claranet Santé

18-20 rue du Faubourg du Temple

75011 Paris

FRANCE

2. Gateway Service Provider (Only for END USERs using the Gateway service)

Seeburger AG

Edisonstrasse 1

75015 Bretten

GERMANY

APPENDIX 3: Hosting of the Software Package

1. Type of Host

The host is an "HADS" and ISO 27001 host. **HADS** stands for "**H**ébergeur **A**gréé **D**onnées de **S**anté à caractère personnel" which ensures the Customer a very high level of security and confidentiality concerning the data it handles.

The data is hosted in a TIER III plus data center, guaranteeing minimum 99,982% availability.

2. Back up of the data

The SERVICE PROVIDER uses dedicated servers for Production, Backup and Safety via the host.

The data are automatically saved in a second safe site (distant back up) every week day. Monthly backups and annual backups are also operated by the host and are saved for 2 years and 5 years respectively.

The backup system is managed by Standard Operating Procedure and tested every year by the SERVICE PROVIDER.

3. Disaster Recovery Plan

A disaster recovery system dedicated to the SERVICE PROVIDER is in place and the system is replicated each 2 hours all days on a Safety server. The Disaster Recovery Plan is managed by Standard Operating Procedure and tested periodically by the SERVICE PROVIDER.

In case of failure of the service due to a failure of the host, the SERVICE PROVIDER commits to restore the service in less than 2 hours.