

# SOFTWARE AS A SERVICE (SaaS) CONTRACT

## MEMORY

This SOFTWARE AS A SERVICE AGREEMENT is entered into on [INSERT DATE], (the "Effective Date") between MEMORY, a simplified joint stock company, whose registered office is located at 11-13 Cours Valmy, 92800 PUTEAUX and registered with the Nanterre Trade and Companies Register, under n°920 613 478 ("Memory SAS") and [INSERT CLIENT'S NAME] whose registered office is located at [INSERT CLIENT'S REGISTERED OFFICE ADDRESS] and registered with the RCS of [City] under n°[number] (the "Client").

Memory SAS and the Client are also referred to in this SaaS Contract individually as the "Party" and jointly as the "Parties".

The Parties elect domicile at the addresses mentioned above for the performance of this SaaS Contract and its consequences.

### 1 PREAMBLE

Memory SAS has developed a platform, referred to as the "Platform", which facilitates user experience and protects the services provided, by managing access and the digital identities of the Client's employees, partners, customers and connected objects.

### 2 DEFINITIONS

"High Risk Activities" means an activity, such as the operation of a nuclear facility, aerial navigation or communication systems, air traffic control systems, life support medical devices, or weapons systems where the use or failure of the Services could result in death, physical injury or environmental damage;

"SaaS Contract": means this Software As A Service Contract, the purpose of which is to define the legal, technical, organizational and commercial conditions under which Memory SAS provides the Services subscribed to by the Client;

"Order": means any document signed and accepted by the Parties, containing a description of the Services subscribed to by the Client from Memory SAS, the conditions for activating them, and the associated price and duration;

"Contents" refers to all data, information, files and items furnished by the Client under the SaaS Contract. This includes, in particular, personal data collected, processed or stored as part of the Services and/or use of the Platform;

"Configuration Data" refers to the data resulting from the parameter-setting and/or configuration operations carried out specifically by Memory SAS and/or the Integrator for the Client's needs as part of the use of the Platforms and Services;

"Personal data": means any information relating to an identified or identifiable natural person (hereinafter referred to as the "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 his or her physical, physiological, genetic, mental, economic, cultural or social identity;

"Distributor": refers to the company responsible for marketing and/or renewing the Services for the Client;

"IaaS" (*Infrastructure-as-a-Service*) means an Infrastructure-as-a-Service provided by a Cloud service provider on which the Services are hosted or otherwise used in connection with the provision of the Services by Memory SAS;

"Confidential Information" means any information, Data, document, know-how, technique, plan, specification, prototype, algorithm, method or any other element, regardless of its form (oral, written, digital, etc.), which is disclosed by one of the Parties to the other Party;

"Integrator": refers to the third-party service company, designated by the Client and approved by Memory SAS, responsible for advising on, implementing and configuring the Services;

**"Platform"**: refers to the Platform published by Memory SAS, the purpose of which is to provide Clients with the Services they have subscribed to, relating to digital identity management. The conditions of access to the Platform and the nature of the Services actually subscribed to by the Client are defined in the Order.

**"Data Controller"** means the natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing; where the purposes and means of such processing are determined by Union law or by the law of a Member State, the controller may be designated or specific criteria for such designation may be laid down in Union law or in the law of a Member State;

**"Services"**: refers to the Services provided by Memory SAS, from the Platform and subscribed to by the Client as part of his Order and include, in particular, the activation of the "My Identity", "My Access" and "My-Keys" modules, any modification, adaptation, configuration, interconnection, improvement, addition, extension, translation and any work derived from the latter and/or any other element of the Platform, at the Client's request;

**"Supplementary Services"**: refers to any additional service, in particular consultancy, configuration, parameter-setting and/or change management services, subscribed to by the Client from Memory SAS and covered by a separate service contract;

**"Data Processor"**: refers to any natural or legal person, public authority, department or other body which processes Personal Data on behalf of the Controller and on the latter's instructions;

**"Tickets"**: refers to any request made by the Client via the Client Portal.

**"Users"**: refers to the end users of the Client's Information System.

### 3 PURPOSE OF THE SaaS CONTRACT :

The purpose of the SaaS Contract is to define the legal, organizational and commercial conditions governing the provision of Services by Memory SAS to the Client. The specific terms and conditions relating to these services, service levels, prices, duration and any other special conditions will be specified in the Order(s) for Services agreed between the Parties. These conditions apply to all Orders issued by the Client during the term of the SaaS Contract, unless they are expressly modified in writing and accepted by both Parties. Memory SAS undertakes to provide the Services in accordance with the specifications agreed in each Order and the Client undertakes to pay the associated fees in accordance with the terms set out in the Order.

In the event of any contradiction between the SaaS Contract and an Order, the following order of precedence shall apply: (i) the Order; (ii) any appendix to the Order and any other document incorporated by reference; (iii) these general terms and conditions set out in the SaaS Contract; and (iv) its Appendices.

### 4 CONDITIONS GOVERNING THE PROVISION OF SERVICES AND THE PLATFORM :

**Access to the Platform:** Memory SAS provides the Client with the information required to access the Platform and the Services. This access information will be provided in a confidential and secure manner. The Client is responsible for the safekeeping and security of his access information and undertakes not to disclose them to unauthorised third parties. The Client acknowledges and accepts that Memory SAS may monitor access by the Client and its Users and their use of the Services for the sole purpose of verifying compliance by the Client with the stipulations of the SaaS Contract and the applicable Order.

**Availability and Performance:** Memory SAS will endeavour to ensure that the Platform is available as far as possible and functions optimally. However, Memory SAS cannot guarantee uninterrupted availability due to factors beyond its control, such as network failures or force majeure.

**Integration and Configuration:** The Client acknowledges that the integration and configuration of the Platform will be entrusted to the Integrator, according to the specific needs of the Client. Memory SAS will work with the Integrator to ensure smooth integration and optimum configuration of the Platform in the Client's environment. The Client undertakes to provide all information and specifications required by the Integrator and Memory SAS to facilitate this integration.

**Training and Support:** Memory SAS undertakes to provide the Client with resources and relevant documentation to enable optimum use of the Platform. However, the Client acknowledges that the Integrator will be primarily responsible for User training and support during the implementation of the Platform. The Client agrees to cooperate with the Integrator and to follow the training and guidelines provided to ensure effective and secure use of the Platform.

**Technical support:** Memory SAS undertakes to provide technical support to the Client in the event of technical problems or questions relating to the Platform, directly and/or via the Integrator. Technical support will be provided via a ticket system, a

telephone helpline and/or online support. The Client undertakes to report any incident or problem diligently and to cooperate with Memory SAS and/or the Integrator to resolve such problems as soon as possible.

**Changes and Updates:** Memory SAS reserves the right to make improvements, changes or updates to the Platform. These updates may include new functions, new modules, security patches or other improvements. In the event of any impact on the Client, Memory SAS will inform the Client in advance of the planned updates. Memory SAS will endeavour to minimise any disruption to the use of the Platform during such updates.

**Planned interruptions:** In exceptional circumstances, Memory SAS reserves the right to carry out planned interruptions to maintain or update the Platform. Memory SAS will endeavour to schedule these interruptions outside the Client's peak hours and to inform the Client in advance, except in cases of emergency.

**Suspension of Services:** The Client acknowledges and accepts that Memory SAS may suspend the right to access or use all or part of the Services and/or Users, and/or delete any Client Content: (i) where such access or use or Client Content (x) represents a security risk or is otherwise likely to damage the SaaS Services or (y) infringes or otherwise violates the rights or other interests of a third party, contains illegal or prohibited content or activities, or is otherwise likely to give rise to liability on the part of Memory SAS; or (ii) where Memory SAS is required to do so under applicable legal provisions or pursuant to a judicial or administrative decision.

## 5 OBLIGATIONS OF THE SERVICE PROVIDER :

**Provision of the Platform and Services:** Memory SAS undertakes to provide the Platform and Services in accordance with the terms of the Order signed by the Client.

**Maintenance and Improvements:** Memory SAS will be responsible for the regular maintenance of the Platform, including the application of updates, security patches and functional improvements. The Client will be informed in advance of planned updates that may affect the use of the Platform.

**Data security:** Memory SAS undertakes to implement all necessary security measures to protect Client Data stored on the Platform.

**Incident management:** In the event of an incident affecting the availability, security or integrity of the Platform, Memory SAS undertakes to inform the Client promptly of the situation, the measures taken to resolve the incident and the potential consequences.

**Cooperation with the Integrator:** Memory SAS undertakes to work closely with the Integrator to ensure the smooth integration and optimum configuration of the Platform in the Client's environment.

## 6 THE CLIENT'S OBLIGATIONS :

**Lawful Use:** The Client undertakes to use the digital services platform exclusively for lawful purposes and in accordance with the laws and regulations in force. The Client must not use the platform in an abusive, fraudulent or defamatory manner, or for any other activity that could damage the Supplier's reputation or violate the rights of others.

**Secure Access:** The Client is responsible for maintaining the confidentiality of its identification information (user ID and password) used to access the Platform. The Client must not share this information with unauthorised third parties and must immediately inform the Supplier if there is any suspicion that their identification information has been compromised.

**Compliance with the Conditions of Use:** The Client agrees to comply with the conditions of use of the Platform established by Memory SAS.

**Payment:** The Client undertakes to comply with the payment terms agreed, where applicable, for the use of the digital services platform. Any delay in payment may result in sanctions, including the temporary suspension or termination of the service.

**Suitability:** The Client is responsible for ensuring that the Platform and the Services subscribed to are suitable for its specific needs. Before subscribing to the Services, the Client acknowledges that it has assessed the suitability of the Services and the Platform for its requirements.

**Compliance with the Terms of Use:** The Client undertakes to use the Services and the Platform solely for internal purposes within its organization. Under no circumstances may the Client transfer, resell, distribute, reproduce or make available all or part of the Services or the Platform to unauthorised third parties, whether for commercial or other purposes, without the prior written agreement of Memory SAS. The Client acknowledges and accepts that it will be solely responsible for ensuring that its use and the use made of the Services by its Users does not exceed the limits set out in the applicable Order.

**Responsibility of Users:** The Client is solely responsible for any use of the Services by Users, and must ensure that Users do not circumvent or divulge usernames, passwords or any other access or authentication data, and that they do not interfere with or disrupt the other security control mechanisms of the Services. The Client must guarantee Memory SAS against any recourse by a third party resulting from a breach by the Client or its Users of its obligations under the SaaS Contract.

The Client will be solely responsible for the acts and omissions of its Users as if they were its own acts and omissions, and will be solely responsible for guaranteeing that any person using the Services does so in accordance with the general conditions defined in the SaaS Contract. In particular, the Client undertakes to guarantee that neither it nor its Users: (i) will access the Services or

use them to host or transmit any content, data or information that is illicit or that violates the rights of third parties, such as intellectual property rights or the right to privacy, or that contravenes applicable legal provisions in any other way; (ii) make any copy, translation, derivative work, disassembly, decompilation, reverse engineering or any other attempt to discover the source code or the underlying ideas or algorithms incorporated in the computer applications or other systems used for the provision of the Services (including Infrastructure-as-a-Service - IaaS), except as expressly permitted by applicable law, and will not remove any title or trademark, copyright or other proprietary notices contained in any systems, software or other material used in connection with the provision of the Services; or (iii) access or use the Services in order to create competing products or services by copying their features and user interfaces or by allowing a direct competitor of Memory SAS to access or use the Services.

**Cooperation and Feedback:** The Client will cooperate with Memory SAS and the Integrator by providing constructive feedback to the latter concerning the use of the Services. In particular, the Client will notify Memory SAS immediately upon becoming aware of any breach or risk of breach of this clause, or any known or threatened breach of security, including any attempt by a third party to gain unauthorised access to the systems used to provide the Services.

## 7 PRICES AND TERMS OF PAYMENT

The Client will pay the Price in accordance with the conditions set out in Appendix C and/or in the associated Order. Unless otherwise stipulated in an Order, the Price is payable in the form of annual fees (*'redevances annuelles'*), to be paid in advance, within thirty (30) days of the invoice issued by Memory SAS.

In order to maintain the fairness and viability of the SaaS Contract, Memory SAS reserves the right, including during the Initial Period of the SaaS Contract, to revise the rates applicable to the Services, up to a maximum of 5% (five per cent) over a period of 12 (twelve) months. Where applicable, Memory SAS will inform the Client, including a transparent description of the new rates applicable at least three (3) months before they take effect. Such adjustments will be applied automatically.

The Client expressly acknowledges that price adjustments in accordance with this clause shall under no circumstances constitute valid grounds for early termination of the SaaS Contract.

Any delay in payment (whether partial or total) of an invoice will automatically and without the need for a reminder result in:

- a penalty equal to the latest refinancing rate of the European Central Bank plus ten (10) percentage points on the date of issue of the invoice. The penalty rate is applied to the total amount of the invoice including VAT; it will not be modified until full payment has been made, even if a partial payment has been made in the meantime. Penalties are due from the first day of delay of the invoice concerned until full payment. These penalties are not subject to VAT; and

- a lump sum of forty (40) euros to cover recovery costs. If the collection costs incurred by Memory SAS exceed this amount, the Client will be reimbursed on presentation of proof.

If an invoice is disputed, payment of the disputed invoice remains due. If the dispute is accepted, a credit note will be sent to the Client as soon as possible. Memory SAS also reserves the right to terminate the SaaS Contract, in accordance with the provisions of article 14 below.

## 8 DATA PROTECTION AND SECURITY

As part of the performance of the SaaS Contract, Memory SAS, in its capacity as Data Processor, may process Personal Data on behalf of the Client, acting in its capacity as Data Controller. Memory SAS undertakes to process such Data in accordance with the provisions of Appendix D, relating to the sub-processing of personal data.

The Parties undertake to comply with all the legal obligations incumbent on them with regard to personal data law and in particular European Regulation 2016/679 of 27 April 2016 which came into force on 25 May 2018 (hereinafter, the "GDPR"). Memory SAS

undertakes to provide the Client with a Platform and Services that comply with the principles of personal data protection, enabling the Client to implement its obligations arising from the Regulation ("Privacy by Design" principle).

More broadly, Memory SAS undertakes to comply with its obligations regarding the security and protection of Personal Data.

It therefore undertakes, as part of the performance of the SaaS Contract, to apply appropriate and sufficient technical and organizational measures to ensure the security of the Platform and the Services ("Security by default" principle).

Memory SAS recognizes and accepts that the security of the Platform and Services is an essential condition for the Client.

Memory SAS is responsible for maintaining the security of the Personal Data contained in the Platform, both through its own components and services and through upstream components and dependencies (e.g. libraries, operating environment or third-party APIs).

Memory SAS ensures that the security of the Platform and the Data and Content contained therein keeps pace with technological developments by complying with the standards and reference frames associated with the Platform.

## 9 CLIENT CONTENTS

The Client's Content are the sole property of the Client, and Memory SAS and the Integrator have no property rights over them. The Client remains responsible for the legality and relevance of its Content, and for any authorization required for its use.

As part of the performance of the Services, the Client authorizes Memory SAS to process its Contents and in particular its Personal Data, in accordance with the written instructions sent by the Client, under the conditions defined in the Order and in Appendix D.

The Client grants Memory SAS the non-exclusive right to host, store, process, modify and transfer all or part of the Client's Contents for the sole purpose of performing the Services and/or Additional Services by Memory SAS and their use by the Client. At the end of the SaaS Contract, Memory SAS undertakes to delete the Client Contents as soon as possible, in accordance with the provisions of the SaaS Contract.

The Client acknowledges and accepts that Memory SAS may, for the duration of the SaaS Contract and beyond, use the characteristics, trends and any statistical data resulting from the use of the Services (excluding the Content) for the purposes of developing and/or improving the Services and any other products and services provided by Memory SAS.

## 10 INTELLECTUAL PROPERTY

The Client acknowledges that, with the exception of the Configuration Data, which is the property of the Client, all intellectual property rights relating to the Platform and its components, in particular developments, databases, applications, interfaces, graphic elements, brands and/or any related content, documentation and any support provided by Memory SAS to the Client under the SaaS Contract, are the exclusive property of Memory SAS and/or its licensor(s). The Client undertakes not to copy, modify, distribute, license or attempt to decompile any element of the Platform.

The Client acknowledges and accepts that in the event of a written request to upgrade the Services and if Memory SAS decides to accept and implement such a request, all such upgrades, improvements and/or additions made in response to a Client's request for an Additional Service will be considered an integral part of the Platform and/or of the Services and will be the exclusive property of Memory SAS and/or its licensor(s). The Client acknowledges and accepts that under no circumstances may he/she claim any intellectual property rights over the developments, unless a separate written agreement is concluded between the parties.

Under the conditions defined by the SaaS Contract and the Order signed by the Client, Memory SAS hereby grants the Client, for the duration of the applicable Order, a non-exclusive, revocable, non-transferable and limited right to use and authorize its Users to use the Services.

Under no circumstances shall such a license right (i) constitute a transfer of ownership of the intellectual property rights concerning the Platform and/or the Services to the Client ; (ii) allow the Client to reverse engineer, disassemble, decompile, reproduce, retransmit, recreate, copy, sell, distribute, publish, broadcast, circulate, commercially exploit or sub-license the Services and/or all or part of the Platform (including any modification or derivative work) to a third party, or for any purpose whatsoever; (iii) allow the Client to use the Services beyond strictly internal use, by a prescribed number of Users, as indicated in the Order.

If the Client chooses to provide Memory SAS with comments, suggestions or improvements regarding the Service (collectively "**Feedback**"), the Client grants Memory SAS the right to use, reproduce and incorporate such Feedback into the Service without any obligation of compensation or attribution.

If the Client becomes aware, it must immediately inform Memory SAS of any suspected infringement of intellectual property rights relating to the Services and/or the Platform. Memory SAS reserves the right, at its sole discretion, to take steps to protect its intellectual property rights, including termination of the SaaS Contract in the event of substantial infringement.

## 11 GUARANTEES AND EXCLUSIONS

Memory SAS guarantees that the Services supplied to the Client under the SaaS Contract will essentially comply with the specifications provided in the Order and in Appendix A. This guarantee shall not apply in the event of: (i) access to or use of the Services by the Client or any User which does not comply with the terms of the SaaS Contract, the relevant Order (or any Schedule to that Order), or Memory SAS's instructions; (ii) any modification or change made by any Party other than Memory SAS to the SaaS Services or to the systems, software or other content or equipment incorporated in those services; or (iii) provision of the SaaS Services free of charge or on an experimental basis or in their pre-market or beta version.

The Client shall notify Memory SAS in writing without delay of any non-conformity of the Services, describing it in sufficient detail and at the latest within thirty (30) days of the Client's discovery of the non-conformity.

Unless otherwise expressly stipulated in the Service Level Agreements (SLAs) defined in Appendix B, Memory SAS will make all economically reasonable efforts to correct this non-conformity. If Memory SAS is unable to correct such non-conformity, after having made all economically reasonable efforts to do so for a reasonable period of time, either Party may terminate the relevant Order corresponding to the non-conforming Service(s) by written notice to the other Party, in which case the Client shall receive, as sole and exclusive compensation, reimbursement by Memory SAS of all sums already paid by the Client in payment of the Price, calculated on a pro rata basis for the period of service remaining after the effective date of termination. All other mechanisms provided for in article 1223 of the Civil Code are hereby excluded.

Except as expressly provided in this section, Memory SAS and its licensors make no representations or warranties of any kind, express or implied, statutory or otherwise, with respect to the Services or their component(s). These exclusions only apply in the conditions prescribed by the applicable legal provisions.

**High Risk Activities.** Memory SAS expressly excludes, in its own name and on behalf of its licensors and the Cloud Provider, any express or implied warranty that the Services are suitable for the conduct of High Risk Activities.

## 12 THIRD-PARTY CLAIMS

Memory SAS shall not be bound by any obligation and shall under no circumstances be held liable under article 11.1 in the event of a dispute arising from:

- the Client Contents;
- use of the Services by the Client or its Users after Memory SAS has asked the Client, under the conditions defined in the SaaS Contract, to cease or cause such use to cease and the Client has had a reasonable opportunity to cease or cause such use to cease;
- any modification or unauthorised use of the Services where the breach or misappropriation would not have occurred in the absence of such modification or unauthorised use;
- any use of the Services or any other act committed by the Client or a User which constitutes a breach of the SaaS Contract, where the breach or misappropriation would not have occurred in the absence of such breach;
- any dispute arising from a voluntary infringement in which an unfavorable judgment has been rendered against any person other than Memory SAS or the Cloud Provider;
- any combination of the Services with any other product, service, software, content, data or method not supplied by Memory SAS; or
- any license for free (without fees) or trial license for the Services.

If any part of the Services is infringing or is considered by Memory SAS to be infringing or likely to be found to be infringing, Memory SAS may choose (at its discretion and expense) to: (a) purchase a license to use the (allegedly) infringing material; (b) replace the (allegedly) infringing material with a non-infringing equivalent; or (c) modify the (allegedly) infringing material to bring it into compliance while providing substantially the same level of functionality. If Memory SAS considers that the measures described above are not economically reasonable, Memory SAS will immediately terminate the Client's access to the Services.

The Client (i) will (at its own expense) defend Memory SAS and its licensors in any action brought against Memory SAS by any third party arising out of or in connection with (a) any use of the Services by the Client or its Users in breach of applicable laws or regulations; or (b) any allegation that the Client's Content violates, infringes, or misappropriates the rights of any third party; (c) the use by the Client or its Users of the Services or any other act committed in breach of the SaaS Contract or the Order; or (d) the conduct, by the Client or a User, of High Risk Activities, and ii) pay the amount of damages that Memory SAS has been ordered to pay by a final decision or the amount agreed as part of a settlement of the dispute approved by the Client. The preceding stipulations will apply both when the damage has been caused directly by the behavior of the Client and/or a User and when the damage has been caused by the behavior of a third party using the Client's or a User's access identifiers if the Client has made his identification details available through negligence or has chosen them in such a way that they could easily be pirated.

The present article constitutes the sole and exclusive remedy of the Client and the entirety of the obligations of Memory SAS (and its subsidiaries) towards the Client in relation to any dispute concerning the violation or misappropriation, by the Services, of the intellectual property rights of third parties.

### 13 **LIMITATION OF LIABILITY**

With the exception of (i) damages resulting from death or personal injury caused by gross negligence, wilful misconduct, fraud or fraud attributable to one of the Parties ; and (ii) the right of Memory SAS to recover all sums due in payment of the Price agreed hereunder, the liability of each of the Parties (or of the licensors of Memory SAS) shall under no circumstances, and whatever the nature of the claim, be liable to the other Party or to any other person or entity under this SaaS Contract for damages per calendar year in excess of the total Price paid (annual fee plus the amount due for Specific Services where applicable) during the twelve (12) month period preceding the date of the incident giving rise to the liability.

To the fullest extent permitted by law, neither Party shall be liable to the other Party on any legal ground or under any doctrine of liability, even if a Party has been advised of the possibility of claiming such damages as compensation for indirect, incidental, special, consequential damages, loss of profits or savings, revenues, or customers; damages resulting from business interruption, unauthorized access, alteration or loss of Client Contents.

The Parties acknowledge that the limitations of liability set out in this clause reflect the liability of the Parties under their respective obligations under this SaaS Contract and constitute substantial elements thereof, and that the Parties would not have entered into this SaaS Contract in their absence.

No claim, in whatever form, arising from this SaaS Contract may be brought against the Client more than two (2) years after the Client knew or should have known of the event giving rise to the claim.

### 14 **DURATION AND TERMINATION**

The SaaS Contract will enter into force on the Effective Date for an initial term of at least **three (3) years** (the "**Initial Term**"). Beyond the Initial Term and unless terminated in writing by one of the Parties within a period of three (3) months prior to the expiry date of the Initial Term, the SaaS Contract will be renewed by tacit agreement for successive periods of one (1) year.

Either Party may terminate this SaaS Contract and/or any Order upon written notice if the other Party ceases to carry on business or becomes subject to insolvency proceedings or any other equivalent proceedings in any other jurisdiction, and such proceedings are not terminated within ninety (90) days to the extent permitted by law, or if it is generally no longer able to perform its obligations under the SaaS Contract and/or any Order.

In addition to any other remedies available to a Party at law, in equity, or under the SaaS Contract, a Party may terminate this SaaS Contract and/or any Order after giving prior written notice to the other Party within thirty (30) days in the event of a substantial breach by the other Party of the provisions of the SaaS Contract and/or an Order without remedying such breach (where applicable) within thirty (30) days, including any act or omission by the Client or a User that entitles Memory SAS to suspend the provision of the Services. A substantial breach is defined as a breach which prevents the further performance of the SaaS Contract and/or any Order or which seriously impairs the performance of the Services.

Notwithstanding the provisions of article 1229 of the French Civil Code and by explicit agreement between the Parties, the effects of this termination are only for the future from the date of notification and will not be retroactive. In the event of termination, the Client must pay all amounts due for services provided up to the effective date of termination. The Parties acknowledge that any Services

which have been paid for by the Client or which the Client has undertaken to pay for are recognized as having been useful to the Client.

As an express derogation from the provisions of articles 1224 and 1226 of the French Civil Code, the Parties also agree that, with the exception of the present provisions, the SaaS Contract and/or any Order may not be terminated or cancelled by a simple notification sent by the creditor to the debtor.

On the effective date of expiry or termination of an Order, the Client will terminate access to and use of the Services by the Client and its Users.

## 15 **CONFIDENTIALITY**

Each of the Parties undertakes to use the Confidential Information of the other Party within the limits of what is strictly necessary and for the sole purpose of performing the SaaS Contract. Each of the Parties undertakes to take reasonable measures to protect the Confidential Information of the other Party, provided that these measures are at least as protective as those implemented by the Parties to protect their own Confidential Information of the same nature, and that they are in any event at least equivalent to the degree of diligence that can reasonably be expected.

Each of the Parties may disclose the Confidential Information of the other Party to its employees, co-contractors, licensors or agents who: (a) need to know it under the SaaS Contract, and (b) are legally bound to protect the Confidential Information in a way that is at least as protective as that provided for in the SaaS Contract. In addition, Memory SAS may disclose the Client's identity to its subsidiaries, employees, suppliers, service providers and licensors for the sole purpose of executing the SaaS Contract and Service Orders.

This section shall not apply to information in respect of which either Party can demonstrate that: (a) it was already published at the time of disclosure, or was published shortly thereafter, or entered the public domain through no fault of the Party receiving it; (b) it was already in the hands of the receiving Party at the time of disclosure and was not subject to a prior obligation of confidentiality; (c) it was received after having been disclosed by a third party who had the right to disclose such information (without any corresponding obligation of confidentiality); or (d) it was independently developed by the Party receiving it without recourse to the Confidential Information of the Party disclosing it.

The Party receiving such information will not be considered to be in breach of its obligations under this section if it discloses the Confidential Information of the Party making the disclosure to the extent strictly required by law to comply with a legal obligation imposed by a governmental or regulatory authority, provided that upon receipt of any such request, and to the extent permitted by law, it shall promptly : (i) notify the Party disclosing the Confidential Information before any such disclosure in order to allow that Party to object to such disclosure or to take such other steps as it considers appropriate to protect the Confidential Information and; (ii) take all necessary measures to restrict any disclosure to that necessary to satisfy any legal requirement imposed by any governmental or regulatory authority (including by withholding commercially sensitive information where permitted by law).

Any reproduction of the Confidential Information of the other Party shall remain the property of the Party disclosing such Confidential Information, and the Party disclosing such Confidential Information may at any time, including at the termination or expiration of the SaaS Agreement, request that the Party receiving such Confidential Information return, destroy or delete (and confirm such destruction or deletion) as instructed (and in such a manner that it cannot be recovered) any Confidential Information of the Party disclosing such Confidential Information which is in the hands or under the control of the Party receiving such Confidential Information. Notwithstanding the foregoing, each of the Parties may archive all copies of Confidential Information which it is required to retain in order to comply with legal and other accounting requirements to which it is subject.

The Client also undertakes not to disclose the conditions defined in the SaaS Contract and/or the Order to any third party unless the Parties agree otherwise.

16 **INSURANCE**

Memory SAS declares that it is insured with a notoriously solvent insurance company for all the harmful consequences for which it may be held liable in connection with the performance of the Services. Each Party is responsible for insuring its property, Data and its employees and agents.

Upon request, each Party undertakes to provide the other Party with an insurance certificate attesting that the policies described above have been taken out.

17 **FORCE MAJEURE**

Except the Client's obligation to pay Memory SAS the sums agreed under the SaaS Contract and any Order, neither Party shall be liable for any delay or failure to perform an obligation under this SaaS Contract where such delay or failure was caused by a circumstance or event beyond its reasonable control, including, but not limited to, electrical or power failures, failures of telecommunications equipment or services, earthquakes, storms or any other natural disaster, blockades, embargoes, riots, government intervention by means of measures or decisions, acts of terrorism or war, labor disputes with its employees or those of its subsidiaries, industrial disturbances.

18 **TRANSFER**

The Client acknowledges and accepts that it may not transfer the SaaS Contract or grant a sub-license and/or delegate any of its rights or obligations under the SaaS Contract, including by operation of law, without the prior written authorization of Memory SAS, and any attempt to do so in breach of this article shall be considered null and void. The SaaS Contract is binding upon the Parties, their respective successors and permitted assigns and applicable for their benefit.

19 **END OF CONTRACT AND REVERSIBILITY**

At the end of the SaaS Contract, the following provisions will apply:

Memory SAS undertakes to send the Client, as soon as possible, the Configuration Data and its Contents, in the format agreed between the Parties.

In particular, Memory SAS undertakes to cooperate and to provide all reasonable assistance to the Client and/or its employees to facilitate the orderly liquidation of the use of the Services and/or to ensure the transition of the services to another supplier. During this transition period, the Client undertakes to pay the fees due in respect of the applications connected to the Platform for the duration of the transition. Given the nature of the Services, the Parties undertake to discuss and agree together the technical and commercial terms and conditions (including the amount of fees due) of reversibility, in a separate contract in order to ensure a planned and orderly transition.

If the termination is the result of the Client's failure to comply with the SaaS Contract, Memory SAS will invoice the Client in advance for all support services provided as part of this transition, and the Client will pay in advance the Price so invoiced for these services.

At the end of the Contract and on full completion of the reversibility phase where applicable, Memory SAS will destroy, cause to be destroyed, or otherwise delete the Client Contents in its possession or held by its Cloud provider (including data backups).

The Client's Contents will be stored for a maximum of ninety (90) days following the expiry or termination of the Client's subscription, and Memory SAS will delete the latter, including the Personal Data, unless the applicable legal provisions or the provisions of the SaaS Contract authorize or require Memory SAS to retain all or part of this Content.

20 **SUB-PROCESSING**

The Client acknowledges and accepts that Memory SAS is free to use the sub-processors of its choice to carry out all or part of the Services. Sub-processors may be designated in the Order or any other document. Where appropriate, Memory SAS will inform the Client of the sub-processors selected and will guarantee to the Client that their services are carried out correctly.

The Client expressly authorizes Memory SAS to change sub-processors/suppliers at any time. Memory SAS must inform the Client of any such change at least one (1) month before the change takes place. Memory SAS undertakes to select a supplier offering services that are at least equivalent in terms of performance, so that no change is perceptible to the Client. This change does not give the Client any specific right to terminate the contract, unless otherwise agreed between the Parties.

## 21 **COMPLIANCE WITH LEGAL PROVISIONS**

Memory SAS will comply with all the legal provisions applicable to it and to its activity in providing the Services to the Client and the Client will comply with all the legal provisions applicable to it and to its activity in providing its Contents and using the Services. Each of the Parties will comply, in particular, with the legal provisions applicable to it in terms of the protection of personal data according to the capacity in which it is acting in the context of the processing of the Client's Personal Data, by virtue of the SaaS Contract.

## 22 **PARTIAL NON-VALIDATION**

If one or more provisions of the SaaS Contract are held to be invalid or declared as such in application of a law, regulation or following a final decision by a competent court, the other provisions shall retain all their force and scope. The Parties then agree to replace the clause declared null and void with a clause that is as close as possible in terms of content to the clause initially agreed, and given the initial intention of the Parties, so as to maintain the economic balance of the SaaS Contract. The same principles will apply in the event of incomplete provisions.

## 23 **COMMUNICATION**

The Parties acknowledge and agree that Memory SAS may, subject to compliance with the confidentiality obligations set out above, refer to the business relationship established with the Client for communication and marketing purposes. Such reference may include, but is not limited to, the use of the Client's name, logo and trade name in materials such as the Memory SAS website, promotional materials, case studies and/or presentations. Memory SAS undertakes to exercise this authorization responsibly and to comply with any general communication guidelines provided by the Client. The Client acknowledges that this mutual communication may contribute to the commercial development of both Parties by enhancing their respective visibility. The Parties agree that communication activities must under no circumstances disclose confidential or sensitive Client information. Memory SAS will take all reasonable steps to avoid any inappropriate or harmful use of the Client's information as part of its communication activities. This communication clause remains in force for the duration of the SaaS Contract and continues after its expiration or termination, unless expressly stated otherwise in a written agreement between the Parties.

## 24 **INDEPENDENCE OF THE PARTIES**

None of the Parties may use the provisions of the SaaS Contract to claim the status of agent, representative or employee of the other Party, in order to establish a relationship of subordination between the two Parties. Each of the Parties retains its own autonomy, responsibilities and customers. Memory SAS will carry out the Services in complete independence, whether on its own premises or on the Client's premises. Memory SAS personnel will remain under the authority of Memory SAS and will comply with the instructions given to them by Memory SAS. All the personnel of each Party involved in the SaaS Contract remain under the responsibility of that Party. Neither Party may give orders to the other Party's personnel.

## 25 **CHANGES**

Unless expressly stipulated otherwise in the SaaS Contract, the SaaS Contract may only be modified, amended or extended by a written agreement signed by both Parties.

## 26 **NON-WAIVER**

No delay, negligence or abstention on the part of one of the Parties in exercising its rights to obtain performance by the other Party of the general conditions laid down in the SaaS Contract (i) shall be deemed to constitute a waiver of the exercise of these rights, (ii)

shall under no circumstances prejudice the rights of this Party under the SaaS Contract, and the exercise, even partial, of one of these rights shall under no circumstances preclude any subsequent exercise of these or any other rights.

27 **APPLICABLE LAW AND COMPETENT JURISDICTION**

In the event of any difficulty in the performance of the Order and before implementing the conditions for terminating it, each of the Parties undertakes to first try to find an amicable solution to the dispute between them. To this end, the Parties shall appoint two persons duly authorized for this purpose. These persons will meet at the initiative of the most diligent Party within thirty (30) days of receipt of the registered letter with acknowledgement of receipt requesting the holding of a conciliation meeting. The agenda for this meeting is set by the Party initiating the conciliation. The decisions taken by the Parties during this meeting will be the subject of an amendment dated and signed by the Parties.

IN THE EVENT OF A DISPUTE RELATING TO THE FORMATION, INTERPRETATION, PERFORMANCE OR TERMINATION OF THE ORDER AND IN THE EVENT OF FAILURE TO REACH AN AMICABLE CONCILIATION BETWEEN THE PARTIES WITHIN A MAXIMUM PERIOD OF THIRTY (30) DAYS FROM NOTIFICATION OF THE GRIEVANCES BY THE MOST DILIGENT PARTY, COMPETENCE IS ASSIGNED TO THE COMPETENT COURTS OF STRASBOURG, NOTWITHSTANDING PLURALITY OF DEFENDANTS OR THE INTRODUCTION OF THIRD PARTIES, EVEN FOR EMERGENCY PROCEDURES OR PROTECTIVE PROCEDURES BY WAY OF EMERGENCY INTERIM PROCEEDINGS ('REFERE') OR APPLICATION ('REQUETE').

**IN WITNESS WHEREOF**, the Parties have agreed that this SaaS Contract shall be signed by their respective representatives duly authorized for this purpose and that it shall come into force on the first date mentioned above.

**MEMORY SAS**

BY:

NAME (in block letters):

TITLE:

DATE:

**CLIENT**

BY:

NAME (in block letters):

TITLE:

DATE:

## APPENDIX A

### A-1 DESCRIPTION OF SERVICES

The Client will be entitled to use the SaaS Services consisting of Identity and Access Management on the Memory Cloud platform. The SaaS Services include the following modules:

- Memory Identity Management: **My-Identity**, which includes identity management, provisioning and reporting;
- Memory Access Management: **My-Access**, which includes the single sign-on (SSO) portal, identity federation and reporting;
- Management of Memory second authentication factors: **My-Access** and **My-Keys**, which includes management of third-party second authentication factors (Yubikey, Window Hello, Google Authenticator, ...) as well as a means of enhanced identity authentication in web browsers and on mobiles, offered through **My-Keys Premium**;

The Client will use SaaS Services to access its resources using the following elements:

- “Web applications” resources: web browsers, tablets, mobile terminals.
- “Mobile applications” resources: mobile terminals.

#### Features and functions of the SaaS Services

**Module: Memory Identity Management: My-Identity** enables identity management, provisioning and reporting.

**Identity Creation:** used to define the algorithm that generates connection identities: size, length, etc. and to customize the identity format.

Identities can be created in different ways:

- Online by an administrator or by the user him/herself (self-registration) depending on the Client's security policies defined during the initial configuration phase;
- Mass import from a screen or standard import from a directory. Imports can also be used to activate simulation mode to confirm changes;
- From external authoritative sources (e.g. the HR information system) via web services, APIs or flat-files. The **My-Identity** SaaS Service makes it possible to segment between different logical structures (e.g. business units, project teams, geographical sites) thanks to the use of security perimeters that correspond to the logical entities. Before an account is created, **My-Identity** SaaS Services ensures that all the control mechanisms that have been configured are respected and that the Client's security policies are complied with.

**Identity lifecycle Management:** storage of the Client's identities in a directory in the cloud and lifecycle management of all the identities of all the Client's users, from their creation (on-boarding) to their deletion (off-boarding). This includes the management of user access requests (workflows, notifications, delegation) and the automatic provisioning of user accounts and associated rights to the Client's applications in the cloud and/or on site. All specific users (directors, CISOs, application managers, etc.) involved in the identity lifecycle process and related authorization requests have access to the specific **My-Identity** SaaS Services functionalities via a portal, according to their functional roles. During the initial configuration, Memory can customize this interface (in terms of parameters and graphics) for each Client, according to the needs defined during the configuration phase workshops.

**Role Management:** role and access models are based on business or application functions. A role can be assigned dynamically (based on identity criteria) or manually. A role can be subject to limitations (e.g. a time limit) or have a multi-dimensional form that enables the operational scope of the role to be specified. The form specifies certain elements linked to the model (e.g. the maximum amount of purchases, the geographical area, the types of Contract managed). A publication matrix can be associated with each role (e.g. the security perimeter, any specific authorization processes associated with the role).

**Organization Management:** organization modelling is used primarily for workflow management and delegated administration tasks. **My-Identity** SaaS Services offer the ability to design several types of organization simultaneously via (by way of example) :

- A hierarchical organization;
- A functional organization;
- An organization by entity;
- Geographical organization;
- Project-based organization.

My-Identity SaaS Services also offer several levels of processes, including:

- A company-wide process, applied if no other process has been declared;
- A process at the security perimeter level, enabling a specific process to be run on a given security perimeter;
- A process at role level enabling the role to monitor a dedicated process.

**Self-Service: My-Identity** SaaS Services offer individual management functionalities on its portal or via APIs for end-users, and via operational tools for administrators and support teams. The aim of these functionalities is to enable end-users to register, give their consent, submit an access request or update their data. The end-user can :

- View and manage your profile;
- Apply for registration yourself (self-enrolment);
- Track the status of your application ;
- Manage your password yourself ;
- Set/modify secret questions (or by SMS).

**Identities and Access rights Provisioning:** to create accounts and rights throughout the IS, **My-Identity** SaaS Services offer a number of options, including:

Automatic provisioning:

- A set of ready-to-use connectors for applications hosted on site (listed in the Documentation);
- Several connectors for applications hosted in the cloud (listed in the Documentation) ;
- New connectors can be developed for cloud applications offering a provisioning interface (web services based on SOAP or REST) or support for the SCIM protocol;

Manual provisioning:

- A flat-file is generated for use by the application concerned;
- An e-mail is sent to the application administrator with the necessary information to enable him/her to carry out the required actions;
- The connectors are synchronous and connected to the applications in real time.

**Delegated Administration: My-Identity** SaaS Services make it possible to establish a delegated administration model within SaaS Services in order to:

- ensure that users can designate other users as delegates for certain profile management tasks;
- guarantee that users can designate other users as delegates for certain tasks related to request management.

This principle of delegated administration can be based on several organizational models.

**The Memory My-Access Access Management module** provides access management capabilities and functions, including:

**Application Portal:** the Application Portal (or the "SaaS Services Portal") is a gateway to the Client's applications connected to the **My-Access** SaaS Services. The latter offer an Internet access portal to the applications:

- Web version for PC/Mac.
- Mobile version for Android/iOS

From the Applications Portal, users can directly access the applications for which they have authorization. Browsing between applications is done without having to authenticate each time, via single sign-on (SSO).

**Authentication and Federation:** My-Access SaaS Services can support several forms of SSO:

- SSO based on an Identity Federation, depending on the protocol used: SAML, OAuth, OpenIDConnect, WS-Federation;
- SSO based on login/password replay through the SaaS Services Portal

**My-Access SaaS Services** can support several authentication methods:

- login/password;
- Kerberos;
- Radius;
- X.509 certificate;
- RSA SecurID;
- Federated Identity Management;
- Memory SAS Multi-Factor Authentication (MFA);
- Smart card ;
- OTP by e-mail or SMS (SMS cost extra);
- OATH via Google Authenticator or Microsoft Authenticator;
- Windows Hello;
- FIDO2 for Yubikey key holder;
- WebAuthN.

Memory can easily add **new authentication methods** to support other third-party solutions:

Access management: **My-Access SaaS Services** enable federated identity management to be created, enabling users' identities to be distributed to another IS or an identity to be retrieved from another IS in order to access your applications. **My-Access SaaS Services** can act as an identity provider but can also rely on other identity providers (the Client, Google, LinkedIn, etc.). **My-Access SaaS Services** can also interface with all applications by acting as a service provider, if the latter have SAML, OAuth or OpenIDConnect interfaces.

Adaptive authentication: **My-Access SaaS Services** enable authentication methods to be adapted according to:

- The user's location (inside or outside the company network);
- The terminal used;
- The authorizations held by the user;
- The authorizations required to access the application;
- Mapping between an application and an authentication level.

**My-Access SaaS Services** allow you to dynamically raise the level of authentication within a single application.

Risk-based authentication: **My-Access SaaS Services** can also be used to assess the risk of access based on the criteria below, and to trigger dedicated action by implementing an access policy:

- Time slot;
- IP address, IP reputation, bot detection...;
- Navigation history;
- Identity attributes;
- Browser and OS used;
- ...

Application self-connection portal: My-Access SaaS Services provide a portal for connecting applications according to the federation protocols used. This portal limits the scope of administration to only those federated applications or applications to be federated for which the application owner is responsible. This delegation mode can be based on the organization model set up by the Client or the administration delegation.

**Security features:** My-Access SaaS Services have several on-board security features, such as:

- Defining the duration of an SSO session;
- Storage of passwords in SaaS Services (and the associated security policy) or use of the Client's own internal repository(s) (AD, LDAP, etc.);
- Definition of limited access (with backup password) if the user loses his means of authentication.

- Individual management services for users, enabling them to reset their passwords by e-mail, secret questions or text message;
- Limiting the number of simultaneous sessions.

### **Memory My-Keys second-factor authentication management**

Memory offers a dedicated management interface for second-factor authentication:

- Manage distribution (by assigning roles);
- Manage requests, potentially with a workflow approval process;
- Manage enrolment, re-initialisation and loss of second factors;
- Provide the Client's support centers with the means to reset or manage the loss of second factors.

Memory natively supports the following second authentication factors:

- Devices with window Hello authentication;
- Google Authenticator / Microsoft Authenticator;
- Yubikey key and any factor requiring FIDO2 / WebAuthn;
- Email / secondary telephone for OTP delivery;
- Smart card;
- Devices protected by InWebo.

New second authentication factors can be added if necessary.

### **Multi-factor authentication Memory MFA My-Keys Premium**

Memory Multi-factor Authentication, available as part of **My Keys SaaS Services**, is a multi-factor authentication option. This functionality is based on strong user authentication using soft tokens from different terminals (tablet, smartphone, web browser). This offer includes the Memory My-Keys module for managing other second authentication factors.

One-time passwords (OTP) are generated in several ways:

- A universal OTP generator (the "**Memory App**") for tablets and smartphones, available on all Java-compatible mobile devices. The Memory App is available on application sales platforms (Apple Store, Google Play). The Memory App MFA works both online and offline;
- Online, users receive a push notification on their mobile phone. After entering their personal code, the OTP is generated and sent directly to the authentication server;
- In Offline mode, after entering the personal access code, the Memory App MFA displays the generated OTP, which the user must copy into the authentication form.

A two-factor authentication module for Internet browsers (the "**MFA Browser Module**"): based on Javascript, it does not require any installation on the Client's workstation, allowing the user to authenticate even if he does not have a mobile phone. If the computer has an Internet browser, the MFA Browser Module is launched on the user page, where the user is asked to enter their password. If this step is successful, the MFA Navigator Module generates an OTP which is automatically sent to the authentication server, guaranteeing its validity. The MFA Browser Module works with all HTML5-compatible browsers. The SaaS Services natively integrate a mechanism for managing the registrations of the Client's mobile equipment. The SaaS Services make it possible to define an enrolment system according to the use cases as well as the procedure to be followed. Registration is carried out by scanning a QR code or entering an activation code displayed in the SaaS Services. The MFA Browser Module can be downloaded via a hypertext link in an e-mail or directly from the SaaS Services Portal.

The end user (and the Client's technical support) can manage the embedded browsers and mobile devices registered via the SaaS Services Portal.

The configuration data includes, for My Identity, the organization model, identity model, rights & roles model, delegated administration model, reports ... for My Access, the authentication model, reports, and for My Keys, the multi-factor authentication model.

## A -2 - DEFINITION OF THE INITIAL PERIMETER

### Users authorized to use Memory:

The Client may initially activate the number of Identities specified for the following Users:

- The Users will be the Client's employees and members of staff, its end customers, its commercial partners and any other person who has a commercial relationship with the Client.
- Users will use the SaaS Services to access the Client's applications, modify the rights associated with Digital Identities and submit requests for new role(s) allowing access to different Client applications.

Initially, the Client can activate up to:

- Insert the number of internal Client Identities (employees, service providers, etc.)
- Insert the number of Sales Partner Identities
- Insert the number of Consumer Identities
- Insert the number of Connected Objects

If the Client wishes to activate additional Identities during the Term, it must send Memory an order form based on the Prices set out in this Contract. On receipt of the purchase order, Memory will issue the relevant invoice. This Contract shall prevail over any additional or contrary provision contained in any purchase order, invoice, receipt or other document relating to the subject matter hereof which is not signed by both parties.

### Identity Categories

The Client may use the SaaS Services for the following categories of Identity (the "Identities"):

- Client identities: employee identities (including trainees, temporary staff, service providers, generic accounts, technical accounts);
- Business Partner Identities: Identities of third parties (business partners) with partial access to the Client's information system via the federated identity management mechanism, via a third-party identity provider, or via an identity management interface.
- Consumer identities: identities of end users who access the Client's e-commerce sites or online commercial services. In this case, access to SaaS Services may be via front office APIs or third-party identity providers (social networks, etc.) and via back office reporting and identity management tools for end users accessing public administration sites and other public administration online services and resources. In this case, SaaS Services can be accessed via front-office APIs or third-party identity providers and via back-office reporting and management tools.
- Connected Objects (IoT): to secure access via connected objects using front office APIs and back-office reporting and management tools. In this case, administrators use SaaS Services for administrative and reporting purposes.

### Territory

- SaaS Services and Client data are hosted at: choose between AWS Dublin or AWS Paris or S3NS Parison
- Users will access the SaaS Services from the following location(s): worldwide, subject to the applicable legal provisions on export controls and the limits defined in this Contract.

### Safety and resilience option

- The Client wishes to activate the DRP (Disaster Recovery Plan) option (recovery within 4 hours in another region of a cloud provider from the time the DRP is triggered): Yes / No
- The Client wishes to activate the option of sending traces to its SOC (Security Operation Centre): Yes / No

### Quota: Number of requests

In order to protect the Memory platform from denial of service, the number of requests made per Client on the Memory platform is limited as follows:

- Input: 100 requests / second,
- Output: 100 requests / second,
- Internally, 50 policies of all types/second

Where

- a request is defined by a unitary call to an API (Endpoint) on the Memory platform, either via the Memory platform's graphical interface, or via third-party applications under the Client's responsibility,
- a Memory policy is defined as an object used to perform a data transformation or a business function including an external provisioning action

If the subscribed quotas are exceeded, Memory reserves the right to queue processes that exceed the above-mentioned request quotas.

If greater performance is required, the Client can subscribe to upwardly revised quotas.

## A -2 - CLIENT'S OBLIGATION TO USE

In addition to the other obligations and liabilities of the Client described in the Agreement, the Client shall be obliged to comply with all of the obligations described below (hereinafter jointly referred to as the "**Client Obligations**"). Failure by the Client to fulfil any of its Obligations may affect the provision of the SaaS Services by Memory SAS or the performance of the Additional Services, and Memory SAS shall not be liable for failure to provide the SaaS Services or failure to perform the Additional Services resulting from the Client's failure to fulfil its Obligations.

The Client must maintain the configuration of the network connection between its data centers and the SaaS Services data centers (an IPsec tunnel or any other dedicated connection);

The Client must maintain the configuration of the federated identity management mechanism between its applications (on site or in the Cloud) and the SaaS Services (SAML, WS-Fed, OAuth and OpenIDConnect protocols);

The Client must maintain the configuration of the provisioning of Identities between the supported versions of its applications (on site or in the cloud) and the SaaS Services as described in the interface contracts validated when each Client application is integrated into the SaaS Services;

The Client will only use the supported versions of browsers and mobile operating systems (the supported versions are versions n and n-1 provided that these versions are still supported by the publisher itself);

The Client shall use the SaaS Services only in the manner described in the functional specifications documentation and any subsequent versions thereof;

If SaaS Services use the Client directory in the authentication process, the Client is responsible for the accessibility and functionality of its authentication elements;

The Client is responsible for the quality of its own data (identities, roles, organizations, etc.) that it provides to the SaaS Services;

During the initialization phase, the Client must:

- ensure that the choices and decisions made meet operational needs and user requirements;
- manage its internal resources dedicated to the project and its subcontractors;
- provide Memory SAS with all the prerequisites specified in the Contract, the applicable technical proposal and the interface documents;
- check and validate the documents relating to the deliverables. Memory SAS will use the Client's templates and procedures available, where applicable, for the supply of deliverables. Otherwise, Memory SAS will use its own templates and procedures.

For each application provisioned, the Client must set up an administrator account for Memory with privileged rights. This account will be stored securely in the SaaS Services. This account must be able to be used to create and manage user accounts and associated rights in the corresponding application.

For each Supplementary Service, the Client must define the scope of its requirements, which will give rise to a quotation from Memory SAS.

When supplying Deliverables as part of Supplementary Services, Memory SAS will use the Client's templates and procedures where appropriate, and, if not, will use its own templates.

## APPENDIX B – SERVICE-LEVEL AGREEMENT (SLA)

### Framework and Support for service quality

This Appendix defines certain qualitative criteria designed to measure the performance of the Memoryty platform in the execution of the SaaS Services. Memoryty will use its reasonable endeavors to perform the SaaS Services at or above the defined Minimum Service Levels (MSLs) as set out in Table 1.1 below from the date the Memoryty platform is put into production.

**Table 1.1**

| Element measured  | Definition   | Evaluation  | Frequency of assessment | MSL   |
|---|--|---|-------------------------|---|
| <b>Incident response time</b>   | <p>Response time for the Client to acknowledge receipt of the problem and assign a ticket (including assigning a severity level)</p> <p>Critical Incidents are reported by a telephone call to the <i>SaaS Service Desk</i>.</p> <p>Non-critical Incidents are recorded in the SaaS Services Portal.</p>                   | <p>(Total number of Incidents responded to within the predefined response time / Total number of Incidents reported during the period) * 100;</p> <p>The response period begins as soon as the Incident is reported.</p>    | Annual                  | <p>95% of responses provided:</p> <p>Within one hour for Severity 1 and 2 incidents</p> <p>Within 2 hours for Severity 3 incidents</p> <p>Within 4 hours for Severity 4 incidents</p> |
| <b>Availability of the SaaS Service - Memoryty My-Identity Management</b>                       | <p>Period of availability of the SaaS Service for <b>My-Identity</b> users, unavailability being defined as the impossibility for <b>My-Identity</b> users to access the <b>My-Identity</b> Portal.</p>  | <p>(Total number of hours of availability of the SaaS Service / Total number of hours of planned availability of the SaaS Services) * 100</p> <p>Note: "Scheduled availability" excludes any planned maintenance slots.</p> | Monthly                 | 99.95%  |
| <b>Availability of the SaaS Service - Memoryty My-Access Access Management</b>                  | <p>Period of availability of the SaaS Service for <b>My-Access</b> users, with unavailability defined as:</p> <ol style="list-style-type: none"> <li>(1) <b>My-Access</b> users cannot access the authentication form, or</li> <li>(2) <b>My-Access</b> users cannot successfully use any authentication method</li> </ol> | <p>(Total number of hours of availability of the SaaS Service / Total number of hours of planned availability of the SaaS Service) * 100</p> <p>Note: "Scheduled availability" excludes any planned maintenance slots.</p>  | Monthly                 | 99.95%  |
| <b>SaaS service availability - Management of Memoryty My-Keys second authentication factors</b> | <p>Period of availability of the SaaS Service for My-Keys users, unavailability being defined as the impossibility for <b>My-Keys</b> users to access the My-Keys portal.</p>  | <p>(Total number of hours of availability of the SaaS Service / Total number of hours of planned availability of the SaaS Service) * 100</p> <p>Note: "Scheduled availability" excludes any planned maintenance slots.</p>  | Monthly                 | 99.95%  |
| <b>SaaS service availability - Memoryty My-Keys Premium multi-</b>                              | <p>Period of availability of the SaaS Service for My-Keys Premium users,</p>   | <p>(Total number of hours of availability of the SaaS Service / Total number of hours</p>   | Monthly                 | 99.95%  |

|  |   |  |                                |          |
|--|---|--|--------------------------------|----------|
| <b>factor authentication</b>   | unavailability being defined as:<br><br>(1) <b>My-Keys Premium</b> users cannot access the My-Keys portal, or<br>(2) <b>My-Keys Premium</b> users cannot successfully use the MFA authentication method (browser and mobile).   | of planned availability of the SaaS Service) * 100<br><br>Note: "Scheduled availability" excludes any planned maintenance slots.         |                                |          |
| <b>Recovery Time Objective (RTO) - My-Identity, My-Access, My-Keys, My-keys Premium excluding reporting functionalities</b>                        | Period within which the SaaS Service must be restored following the incident (or interruption)<br><br>The <b>Recovery Time Objective (RTO)</b> is the target time, and a level of service, within which an operational process must be restored following a disaster (or interruption) in order to avoid unacceptable consequences linked to the disruption of business continuity. | (Period during which the "system" becomes available in the SaaS environment) - (Period during which the incident is officially declared) | Per incident (or interruption) | 4 hours  |
| <b>Recovery Time Objective (RTO) – Reporting features of My-Identity, My-Access, My-Keys, My-keys Premium</b>                                      | Period within which the SaaS Service must be restored following the incident (or interruption)<br><br><b>Recovery Time Objective (RTO)</b> is the target time, and a level of service, within which an operational process must be restored following a disaster (or interruption) in order to avoid unacceptable consequences linked to the disruption of business continuity.     | (Period during which the "system" becomes available in the SaaS environment) - (Period during which the incident is officially declared) | Per incident (or interruption) | 24 hours |
| <b>Maximum Allowable Data Loss (Recovery Point Objective -RPO) - My-Identity, My-Access, My-Keys, My-keys Premium excluding reporting features</b> | Time at which data must be recovered when the interruption occurs.<br><br><b>Maximum Allowable Data Loss (RPO)</b> refers to the amount of data at risk. It is determined by the time elapsed between each data protection measure and reflects the amount of data likely to be lost during incident recovery.  | (Date and time when the "system" became unavailable) - (Date and time of the last backup)  | Per incident (or interruption) | 4 hours  |
| <b>Recovery Point Objective (RPO) – Reporting features of My-Identity, My-</b>   | Time at which data must be recovered when the interruption occurs.  | (Date and time when the "system" became unavailable) - (Date and time of the last backup)  | Per incident (or interruption) | 24 hours |

|   |  |  |  |  |
|---|--|--|--|--|
| <u>Access, My-Keys, My-keys Premium</u> | <b>Maximum Allowable Data Loss (RPO)</b> refers to the amount of data at risk. It is determined by the time elapsed between each data protection measure and reflects the amount of data likely to be lost during incident recovery. |  |  |  |
|---|--|--|--|--|

When an Incident affecting the SaaS Services occurs, the Client shall immediately report the Incident to Memory by creating an Incident file on the SaaS Services support website ("**the Support Site**"). The Support Site records any Incident reported 24 hours a day, 7 days a week. When reporting the Incident, the Client will provide all the details necessary to help in taking action, identify the source and resolve the Incident.

Memory SAS will, at its discretion, diagnose whether the Incident was caused by the SaaS Services or by an external factor. If the Incident was caused by an external factor, Memory SAS will provide reasonable assistance to the Client to remedy the Incident, but Memory SAS will not be responsible for the resolution of the Incident.

If the Incident is caused by SaaS Services, a priority level will be assigned to the Incident based on the defined SLA criteria. In this case, the following procedure will apply:

- Acknowledgement of receipt of the ticket describing the Incident and assignment of a priority level;
- Gathering useful information to take action and try to identify the source;
- Comparison of data with any antecedents in the knowledge base;
- If the source is identified, a corrective measure and a timetable are proposed to the Client;
- If this is not the case, an escalation procedure is initiated for the R&D teams (3<sup>rd</sup> level assistance) in order to find the source. In the meantime, a workaround solution will be proposed, if necessary, to ensure continuity of operations until the Incident is resolved;
- Closure of the Incident file.

Each Incident will be tracked by the Client and Memory SAS on the Support Site, which records when the Incident was reported, additional details provided by the Client, attempts to resolve the problem and any other information until the Incident file is closed.

Depending on the impact of the problem on SaaS Services in the production phase, Memory SAS may, at its discretion, initiate a crisis management procedure in which the Client will be involved.

**SaaS Quality of Service Level - Support:**

The support time slot under the SLA for Severity 2, 3 and 4 Incidents is as follows ("**Support Hours**"):

- 08:00 - 20:00 CET from Monday to Friday (except public holidays in France)
- Any Incident of severity 2, 3 and 4 occurring outside Support Hours will have the corresponding service level agreement (SLA) applied from the next working day during Support Hours (for example, if a Incident of severity 3 is reported on a Sunday, the response time for an Incident defined as an SLA will run from the following Monday at 8:00 CET).

Support in the event of a Severity 1 Incident is on-call (*'d'astreinte'*) during the hours when the Applications are "available" (as defined below).

The SaaS Service Level Agreements (SLAs) and their evaluation methods as defined in this Appendix will be used by Memory to measure its performance in relation to them.

Memory SAS will keep detailed information on its performance used to calculate each SaaS service level agreement (SLA) over 12 rolling months in addition to the current month.

SaaS service levels (SLAs) affected by any change in the service levels agreed with the Cloud provider will be subject to change by Memory SAS.

## Reporting on the performance of Service Level Agreements (SLA):

Memory SAS will provide the Client with a monthly SaaS Service Level Agreement (SLA) performance report so that the Client can check Memory SAS' performance and compliance with SaaS SLAs; this report will identify:

- Service Level Agreements (SLAs) for SaaS services respected;
- Service Level Agreement (SLA) failures for SaaS services;
- Memory SAS will identify the corrective measures taken or to be taken to remedy the cause of the SLA Failures of the SaaS Services.

## SaaS Service Level Agreement (SLA) - Exclusions

A problem will not be considered an SLA Failure of the SaaS Services or a breach of the terms of the Contract (e.g. warranties provided) by Memory SAS if that problem is caused by:

- a) Any non-compliant use of SaaS Services (which does not comply with the guidelines or documents provided by Memory SAS);
- b) Connectivity problems beyond the reasonable control of Memory SAS;
- c) Errors in equipment, softwares and networks beyond the reasonable control of Memory SAS;
- d) A Denial of Service or similar attack aimed at "saturating" a website with requests for information, content or responses;
- e) Failure of applications, code, third-party equipment and any associated interfaces not supplied by Memory SAS;
- f) Malware or any other disabling code not detected by economically reasonable anti-virus protection;
- g) A Force Majeure event;
- h) Any failure by the Client (or any third party supplier, employee, agent or co-contractor of the Client or any other person having access to Memory SAS SaaS Services using the Client's passwords or equipment) to fulfil its obligations under the Contract or any act, error, omission or breach of the Contract if such failure, act, error, omission or breach results in a failure to comply with the quality of service levels (SLA) of the SaaS Services;
- i) Failure by the Client to provide the information or data requested, or failure by the Client to cooperate within a reasonable timeframe, having regard to the service quality levels (SLA) of the SaaS Services;
- j) Intentional fault on the part of the Client or the Client's third-party suppliers, or failure by the latter to comply with the applicable legal provisions;
- k) Requests with response times that are shorter than our maximum response times as defined in the Technical Documentation;
- l) Failures caused by the Client's application logic, by code errors specific to the Client's site, or by errors in the Client's Contents;
- m) Continued use of the SaaS Services by the Client after Memory SAS has recommended that the Client modify its use of the SaaS Services, if the Client has not modified its use in accordance with the recommendation made to it;
- n) Errors in the Client's IP or Client Contents, if these errors are the cause of the problem; or
- o) One or more parts of the SaaS Services that have been expressly identified as test services or beta versions.

Memory SAS shall not be responsible for remedying problems with the SaaS Services caused by the above, and the Client shall reimburse Memory SAS for any costs incurred in investigating problems caused by the Client's Contents or IP, if the origin of the problem is not a SaaS Service. On request, Memory SAS will provide assistance to the Client to remedy these problems, in which case the Client will pay Memory SAS the price agreed between the parties or set out in the article herein relating to Prices.

## Definitions

**"Content"** means knowledge objects, including but not limited to data models, dashboards and queries.

**"Incident"** (i.e. a service management "Incident" according to the ITIL v3 document) means "an unplanned interruption to an IT service or a degradation in the quality of an IT service".

- An Incident is the initial notification of the occurrence of an unforeseen event. An Incident is typically related to a single request or policy. Multiple Incidents can be reported for the same Problem.
- An Incident is "resolved" as soon as (A) any data in the production phase that needs to be corrected has been corrected; (B) a "Problem" is reported, if applicable; and (C) the Incident itself is updated with details of its resolution.

**"Problem"** according to the ITIL v3 document means "the cause of one or more Incidents. The cause is often unknown at the time a Problem File is created, and the Problem Management Procedure allows further investigation".

- A Problem is "resolved" as soon as (A) the origin is identified; (B) the origin is definitively corrected either in the SaaS Services or in the Client's software or infrastructure; (C) the patch is scheduled to be put into production; (D) the version put into production is communicated to the Client; and (E) the Problem File is updated with details of its resolution.

"Availability" - the Applications are expected to be available:

- 24 hours a day, 7 days a week, except during maintenance periods (as defined below)

"Unavailability" - the following elements are excluded from the monthly assessment of availability under the SLAs

- Client network failures
- Authentication problems for which the Client is responsible
- Regularly scheduled maintenance slots
- Periods of unavailability caused by an event of force majeure

"Maintenance slots" making the system unavailable will be limited to two operations per year and a maximum interruption period of 4 hours. These maintenance operations will generally be scheduled outside office hours. Clients will be notified one month in advance by e-mail of any upcoming maintenance operation of this nature. In addition, any operation carried out for security reasons may be subject to maintenance. In this case, Memory SAS will do its best not to affect the SaaS Service. If the SaaS Service is affected, a maintenance operation for security reasons will be considered as a Maintenance Slot. In the case of maintenance operations carried out for security reasons, Memory SAS may reduce notification times as necessary.

"SaaS Services SLA Failure" means Memory SAS's failure to meet a defined service level agreement (SLA) for the SaaS Services. The "Severity Level" classifies the seriousness of an Incident. The following table defines the four levels of severity:

**Table 1.2**

| Severity level                                   | Definition  |
|--|---|
| <p><b>Critical impact / Level 1 severity</b></p> | <p><b>Level 1 Severity - Critical Impact</b></p> <p>Severity 1 incident:</p> <ul style="list-style-type: none"> <li>(1) completely prevents end users from using the SaaS Service(s), or</li> <li>(2) prevents the Client from carrying out critical transactions or critical operational processes.</li> </ul> <p>For Severity 1 incidents, a significant proportion of end users and sites must be affected.</p> <p>For Severity 1 Incidents, there is no economically reasonable workaround for the Client.</p> <p>Examples include:</p> <ul style="list-style-type: none"> <li>• most (or all) end users cannot access the SaaS Service - the VPN is down</li> <li>• end users can access the SaaS Service but most (or all) end users cannot access the search heads - all search heads are down.</li> <li>• end users can access the SaaS Service but most (or all) end-users cannot search 100% of the data stored - impossible to search 100% of the data.</li> </ul> |
| <p><b>Major impact/ Level 2 severity</b></p>     | <p><b>Level 2 severity - Major impact</b></p> <p>Severity 2 incident:</p> <ul style="list-style-type: none"> <li>(1) substantially prevents end-users from using the Service(s) but does not prevent the Client from carrying out critical transactions or critical business processes, or</li> <li>(2) totally prevents a limited number of end users or sites from using the Service(s) or</li> <li>(3) causes a degradation in the performance of the Service(s) which renders the software unusable within economically reasonable limits.</li> </ul> <p>For Severity 2 incidents, a significant proportion of end users or sites must be affected.</p> <p>For Severity 2 Incidents, there is no economically reasonable workaround for the Client.</p> <p>Examples include:</p>  |

|   |  |
|---|--|
|   | <ul style="list-style-type: none"> <li>• individual end users cannot use the SaaS Service</li> <br/> <li>• end users are unable to perform essential key functions within the Services (e.g. inability to access log data or perform security incident searches due to inability to access or use the search function).</li> </ul>   |
| <p><b>Moderate impact/ Level 3 severity</b></p> | <p><b>Level 3 severity - Moderate impact</b></p> <p>Severity 3 incident:</p> <ol style="list-style-type: none"> <li>(1) includes any Incident that would have qualified as a Severity 1 or 2 Incident but for which there is an economically reasonable workaround, or</li> <li>(2) reasonably prevents end users from using the Services but does not prevent the Client from carrying out critical transactions or critical business processes,</li> </ol> <p>For Severity 3 Incidents, a reasonable or limited proportion of end users or sites must be affected.</p> <p>For Severity 3 Incidents, there is a workaround solution that is economically reasonable for the Client.</p> |
| <p><b>No Impact / Level 4 Severity</b></p>      | <p><b>Level 4 severity - No impact</b></p> <p>Severity 4 incident:</p> <ol style="list-style-type: none"> <li>(1) Little or no restriction on use of the Service by end users</li> <li>(2) No impact on critical transactions or operational processes,</li> </ol> <p>For Severity 4 Incidents, a small proportion of end users must be affected.</p> <p>For Severity 4 Incidents, there is a workaround solution that is economically reasonable for the Client.</p>  |

## APPENDIX C - PRICES

The annual subscription fee for the Services depends on the number of Users defined above for Memory Identity Management, Memory Access Management and Memory Multi-factor Authentication respectively.

### Identity count:

The My-Identity and My-Access offers are invoiced on the basis of the number of active identities stored.

An active identity is defined as an identity whose status is set to "Active" and which has a role (excluding the administration role) or has authenticated to an application protected by the Memory platform.

The My-Keys offer (including Premium) is invoiced on the basis of the number of active identities that have started a second authentication factor enrolment process.

The annual number of identities used for billing each offer is calculated as follows:

- Each day, the number of active identities is calculated according to the definition given above,
- For the monthly count, the day with the highest peak of active identities is used for the month,
- For the annual count, the month with the highest peak of active identities is used for the year.

### Price per Identity:

The price is calculated on the basis of the unit rate detailed below (in Euros, excluding VAT):

- Price per Client Identity
- Price per Commercial partners identity
- Price by Consumer identity
- Price by Connected Objects (IoT) identity.

On the effective date, Memory will invoice the Client for the annual subscription fee for the services of .... excluding VAT Euros for year 1.

At the end of the year, if the number of identities recorded exceeds the number subscribed, the subscription will be adjusted.

For year N+1, the subscription commitment is at least the average number of identities recorded for year N.

Additional charges based on usage will be invoiced on each anniversary date.

The initial commitment begins on the Effective Date for an initial minimum term of **three (3) years**.