GENERAL TERMS AND CONDITIONS OF THE "ELECTRONIC DATA ARCHIVING" (EDA) SERVICE

Article 1. PREAMBLE

To promote electronic data sharing as a means of communication in business and administrative affairs, and in order to ensure the durability and ease of retrieval of said data, Docaposte Arkhineo offers a legally recognised electronic archiving service for Electronic Documents under the brand name Arkhineo. The Archiving operation (hereinafter referred to as the "Service") involves collecting the information, storing it in its original format, allowing it to be consulted on request, and retrieval.

This document specifies the terms and conditions that govern the Client's use of the electronic document archiving Service via the Application.

For the avoidance of doubt, the Parties accept and acknowledge that in relation to the Service provided and in respect to the applicable Data Protection laws (GDPR) :

The Client is Data Controller;

The Reseller is Data Processor;

Docaposte Arkhineo (The Company) is Data SubProcessor.

Article 2. DEFINITIONS

Application: A service operated by Docaposte Arkhineo which the Client uses to access the EDA Service.

Application Administrator: the entity responsible for managing the access rights of Authorised Users to the Application's features and functions.

Archive: an Electronic Document received by the Company that has been allocated a UAI. The Archive serves as a basis for invoicing.

Archive Object: an Electronic Document that is being archived.

Archiving: the operation which includes receiving an Electronic Document sent by the Client, storing it in its original format, and enabling it to be Consulted and Retrieved.

Authorised User: a physical person who has been authorised by the Client to make requests via the Application on behalf of that Client.

Client: the legal entity having ordered the EDA Service from the Reseller.

Company: means Docaposte Arkhineo.

Compartment: means an Archive space dedicated to a specific Client.

Consultation: means the different methods the Client may use to consult their Archives.

Contract: the General Terms and Conditions.

Deposit: means the operation whereby an Archive received from a Client is preserved and retrieved in its entirety.

Destruction: is a technical procedure used to ensure the complete and logical destruction of all or part of a Client's Archive held by the Company, at the Client's express request.

Download Log: the legally probative document which catalogues Archives in chronological order. This log is accessible by the Client via the Application for the purposes of checking Uploads.

EDA Service: the Electronic Data Archiving system identified as "the EDA Service", including Transfer and Consultation functions.

Electronic Document: a set of structured computerized data sent by the Client. This set of data may contain more than one file and is intended to be kept by the Company as is, whether the set consists of data or application programmes and whether the data are interpretable or not.

Format: the original format of Electronic Documents received from the Client, without the Company being able to modify it.

General Terms and Conditions (hereinafter GTC): this document.

Identification: the procedure the Client's Authorised Users identify themselves and are recognised by the Company.

Integrity: a property which guarantees that the Electronic Document has not been modified by the Company and that it is stored in its original Format.

Metadata: a structured set of technical, management and description data attached to a document which describes the features of this document in order to facilitate locating, managing, consulting, using or preserving that document.

Network Service Provider: the third-party entity who transfers the data and provides related electronic services between the Parties.

Patient: The owner of the Personal Health Data.

Personal Health Data*:* personal data about the physical or mental health of a physical person, including data about the provision of healthcare services, which reveals information about the state of that person's health (per article 4 ᵖ15 of EU Regulation 2016/679 of 27 April 2016).

Purchase Agreement: the order form and any other document between the Client and the Reseller which relates to the purchase of the EDA Service from the Reseller by the Client.

Purchase Order: an online or paper-based order document established between the Client and the Reseller, specifying the EDA Service ordered by the Client from the Reseller. In the event of a dispute relating to the ordered EDA Service, the terms and conditions of the Service, product descriptions or any other applicable subscription term or condition (for example, the start and end dates of the order), arising between a Purchase Order and the relevant purchase order between the Reseller and the Company, the disputed terms of the Purchase Order between the Reseller and the Company shall apply to the Client.

Reseller: means an entity that has contracted with Company or one of Company's authorized distributors to resell EDA Service and with which Client has contracted directly to purchase applicable EDA Services.

Retention Period: means the period during which the Company agrees to retain an Archive in its system.

Retrieval: the process by which the Client asks the Company to return one or more Archives on an external medium, including at the end of contractual relations, in order to ensure reversibility.

Reversibility: the process of retrieving all Archives.

Security token: a confidential code generated by the EDA Service, allocated to a Client, and enabling the Client to be identified and authenticated in its exchanges via the Application.

Storage Period: the period during which the Company agrees to store an Archive in its system.

Time-stamping: a process by which the Company marks each incoming Electronic Document with a precise GMT time-stamp, using GPS.

UAI (Unique Archive Identifier): an automatically-generated code assigned by the Company to each Archive, identifying it in a unique and permanent manner, and providing proof of the deposit of an Electronic Document.

Uploading: a Client activity which consists of using the Application to entrust the Company with an Archive Object and its associated Metadata.

Upload Log: means the document with legal value listing the Archives chronologically. This log is accessible by the Client in the Application for the purposes of checking Uploads.

Article 3. OBLIGATIONS OF THE COMPANY

The Company declares that Archiving is done on servers located exclusively within the territory of the European Union and in several data centres. The Electronic Data Archiving (EDA) service is based on a technical architecture made up of the sites described below.

Active Archiving site 1 consists of the following elements:

- Technical provisions to provide collection for the Electronic Documents submitted by the Client, as well as Archive Consultation. Uses a dedicated telecommunications access.
- A primary high-availability Archiving unit, in which each Archive is subject to double Archiving on two separate devices.

Active archiving site 2 is located more than 300 metres away from active site 1 and on a different geological level, and consists of the following elements:

- A secondary high-availability Archiving unit, in which each Archive is subject to double Archiving on two separate devices.

The Backup site, located more than 400 kilometres away from active sites 1 and 2, comprises the following elements: a daily backup copy of each collected Archive.

Each of these three sites is located in secure buildings owned by Caisse des Dépôts et Consignations. These sites contain anti-intrusion security equipment, fire detection and extinction equipment, temperature control, and a backup power supply with emergency units.

The Company agrees as far as possible to implement and maintain physical and computer procedures, as well as security measures, designed to protect the data against destruction, loss of integrity or

breach of confidentiality, within the limits of the most recent technical means available and on the condition that the Client complies with technical requirements.

These procedures are intended to ensure that an Electronic Document received by the Company is archived in its original format and that it will be stored in a manner enabling its Consultation and possible Retrieval.

The EDA Service is provided by the Company in compliance with AFNOR standard NF Z 42-013 ("Specifications relating to the design and operation of computer systems with a view to the preservation and integrity of documents stored in these systems").

In this respect, the Company confirms that it obtained NF 461 - Electronic Archiving System certification on 05/02/2019 under number 70331.4; the latter certifies an Electronic Archiving System's compliance with AFNOR standards NF Z 42-013 and ISO 14641-1.

As an Archive depository, the Company is obligated to fully retrieve all archived Electronic Documents on behalf of the Client. For all other Service provisions apart from Archive Retrieval, namely Uploading and Consultation, the Company undertakes to provide these services, which are not strictly-speaking part of the deposit agreement, on the basis of a best-efforts obligation, in accordance with the service levels set out in article 8.

In compliance with applicable legislation, the Company archives and stores all Electronic Documents received and takes all required security measures intended to monitor the Integrity of those Electronic Documents.

The Company implements all the necessary means to ensure the performance and availability of the EDA Service. However, as a general rule, the Company does not warrant that they Application shall be free or errors or failures, nor that the EDA Service will operate without interruption. The Company's liability excludes all Client equipment and infrastructure as well as the equipment and infrastructure of the third party platform.

Article 4. OBLIGATIONS OF THE CLIENT

4.1 Access management

The Client is solely responsible for accessing the EDA Service, specifically with a view to preserving the confidentiality of the access codes and passwords assigned to it.

The Client accesses the Service using authentication methods and passwords assigned in accordance with the procedure determined during the implementation phase of the Service, or through the MyArkhineo portal.

For the purpose of accessing the Service via the MyArkhineo portal, the Client remains solely responsible for use of its means of authentication and its passwords. Any loss or fraudulent use of authentication methods or passwords must be reported by the Client to the Company as soon as possible. Any access to the Service made using the authentication procedure, specifically using the Client's passwords, is deemed to have been carried out by the Client as long as any fraudulent use was not reported to the Company in compliance with the applicable procedures at that time.

The Client may use specific protection methods for all or part of the archived information, such as an encryption method, insofar as no legal or regulatory provision prohibits it. In this event, the Client shall

be fully and solely responsible for ensuring the safekeeping of the keys required to decrypt the information.

The Client acknowledges that only the users authorised by the Application Administrator have access to the Application's archiving functions. The Client vouches for the compliance of its Authorised Users with the confidentiality and security of the means of access to the Application.

4.2 Archiving Format and technical requirements

Electronic Documents are stored exclusively in their original format, and the Client is solely responsible for the selection of electronic formats and their durability.

The Company recommends the Client uses standard, standardised and durable formats; these formats are listed in the document E-MA-20_LISTE-FORMATS provided by the Company.

If the Client chooses one or more formats from this list, the Company will be able to apply a validation process to the format of each Electronic Document entrusted by the Client, reject any invalid Electronic Documents according to the terms specified in the Company's Archiving Policy.

Should the Client select, under its own responsibility, one or more formats that are not on the list of recommended formats, the Company will be able to store them in line with the contractual commitments stipulated in these GTC, but will be unable to validate them when the Client uses the Uploading function.

Furthermore, on this last point, the Company wishes to emphasise that using non-standard formats is likely to affect the documents' durability in terms of long-term readability.

With this in mind, the Company notes that Electronic Document formats are, by their very nature, in a state of evolution. It is therefore the Client's responsibility to preserve the software used to read the relevant files, if needed to use the Archives during their Consultation or possible Retrieval, and to have available to it the competences required for such operations.

Given that it does not have access to the content of the Electronic Documents, the Company states that it is not able to detect or remove any viruses that may be contained within the Electronic Documents.

The Client acknowledges that the Company accepts no liability with respect to the content, nature or features of the archived Electronic Documents. On this basis, the Client guarantees the Company against any claim or third party action relating to the content, nature or characteristics of the Electronic Documents.

The Client may use specific protection methods for all or part of the archived information, such as an encryption method, insofar as no legal or regulatory provision prohibits it.

In this event, the Client shall be fully and solely responsible for ensuring the safekeeping of the keys required to decrypt the information.

On a more general level, the Client agrees that it shall fulfil all present or future obligations it may have relative to the law, regulations, legal rulings, professional standards, jurisprudence, regulatory authorities and applicable codes of professional ethics, and that its Authorised Users shall fulfil the same.

The Client is responsible for ensuring that it has at its disposal the environment and operational equipment required to implement the EDA Service.

Article 5. DESCRIPTION OF THE EDA SERVICE

The Client acknowledges that the Application runs on Docaposte Arkhineo's technical platform. Thus, prior to the activation of the EDA Service, the Client acknowledges having read and accepted the terms of the subscription agreement relating to Docaposte Arkhineo's technical platform.

5.1 Technical and functional specifications of the EDA Service

The Client area is comprised of a dedicated compartment within the archiving space provided for all the clients of the Application. This Client area is created when the Application is activated by the Client.

When Uploading an Archive Object, an Authorised User uses the Application to upload the Archive Object in question as well as its Metadata.

During the Archiving process, an Archive is created and secured within the Client's compartment. When Uploading an Archive Object, a UAI is attributed to that object (consisting of a string of 41 characters, the first 17 characters representing the date and time of the deposit). This UAI's validity is guaranteed throughout the Archive's storage period.

A Documents is uploaded using the Application and secure network access. A successful Upload generates the creation of a UAI.

Metadata includes the fields from attachments and the object to which the attachment is associated. Metadata is used to search the Archives.

Sealing is also a specific component of an Archive. It relates to a file in the XAdES format. It includes imprints for each of the following structures:

- The Archive Object

- Application metadata

- Descriptive metadata

It also includes a link to the previous Archive. This link is made up of the previous Archive's UAI and its seal imprint. The Archive seal also includes data on the deposit (depositor, depositor IP address, protocol used).

Searching for and extracting an Archive can be done in two ways. The first way is to use the Application to carry out a search within Archive Objects. The second way, if activated, is to use the MyArkhineo portal.

With respect to proof of Archiving, Authorised Users can use an Application function to request the creation of a proof of Archiving associated with a specific Archive. This proof includes all the technical elements regarding the Archive's security and integrity. The Company guarantees the traceability of the archiving operations.

Moreover, the EDA Service guarantees the continuous traceability of archiving operations.

5.2 Limitations

The Company undertakes to store the Client's Archives in accordance with standard professional practices.

The Company shall not be considered as a consulting company and shall not incur any liability in the computer or network settings selections made by the Client under its sole and entire responsibility, with the assistance of an IT service provider that it has freely chosen if applicable.

Similarly, as the Company is not a telecommunications network services provider, it shall not accept any liability for any malfunctions related to the technology used by the Client, nor for malfunctions of any kind attributable to the third party technical platform.

Article 6. FINANCIAL CONDITIONS

The Client shall abide by the terms of the Purchase Agreement. The Client acknowledges that adhering to the terms of the Purchase Agreement is a primary condition of this contract. If the Reseller should inform the Company that the Client is breaching the Purchase Agreement, the Company may decide that the Client has breached this contract.
Therefore, the Client undertakes to make payment for invoices submitted by the authorised Reseller in accordance with the terms set out in its agreement with said Reseller.

Any late payment of invoices on the part of the Client shall lead to the following, 15 (fifteen) days after a formal notice has failed to have effect:

- the suspension of Archive consultation;
- after 30 (thirty) calendar days, the suspension of the Uploading function for any new Electronic Document.

The Client further states and agrees that, in accordance with the legal terms applicable to the deposit contract, if the Client fails to make full payment for all outstanding invoices, the Company may, especially in the case of a dispute with the latter, exercise its right of retention with respect to any request for Retrieval of one or more Archives, said right of retention being valid with respect to Parties, even third parties, including any entity responsible for collective insolvency proceedings.

Article 7. ARCHIVING PERSONAL HEALTH DATA

This article applies only to personal health data that may need to be hosted by the Company. The Company states it has received the "Personal Health Data host" official certification from French Health Administration.

7.1 Obligation to inform the subject of the data

The hosting of Personal health data and the procedures for accessing and sending it are governed by a duty to inform the subject of the data. Persons whose personal health data is being hosted must be informed that their data will be stored by a health data hosting service and that they are entitled to forbid their data from being entrusted to a health data hosting service.

Given the exclusive jurisdiction the Client has in gathering and generating personal health data in the course of its activities, the Client is responsible for informing the relevant subjects of that data. The Client undertakes to fulfil this obligation this for the persons in question.

The Company shall inform the Client in the event that it detects any serious incident resulting in the unauthorised disclosure or alteration of this data.

As it is responsible for the processing of the data, the Client shall implement procedures to report serious incidents to the persons whose data it is, and those persons shall be able to access their data and/or correct it in accordance with the procedures described below.

7.2 Right of access and correction

In accordance with the terms of the GDPR, the end user may exercise his or her right of access and correction with respect to the Client responsible for processing.

However, acting as a sub-contractor, the Company shall provide a secure connection with strong authentication procedures exclusively to accessing hosted Personal health data.

The Company does not operate a customer desk service for accessing health data: only End Users may access said data, using strong authentication with a Docaposte Arkhineo certificate.

The Client undertakes to fulfil its obligation to inform the relevant persons of their right to access and rectify their personal data.

7.3 Confidentiality

Personal health data are strictly confidential and are subject to security measures implemented by the Company.

With specific regard to the hosting of personal health data, only the hosting doctor working under a service contract with the Company may access the Archives held by the Company, regardless of the origin of the data and/or its subjects. This access is restricted to the purposes of work performance, as defined in the contract entered into with the Company.

Article 8. REVERSIBILITY

When the contractual relationship between the Client and the Company is terminated, for whatever reason, the Client may request the return of the Archives, on the three following conditions:

- The payment of all sums due to the Company, including amounts linked to the Retrieval request

- The Retrieval request must be expressly made (by registered letter with acknowledgement of receipt) on the effective end date of the contract

- The request must cover all Archives

The Client shall have a period of 30 (thirty) calendar days to retrieve its Archives using the appropriate menu in the Application.

At the Client's express request, Archives can be returned to the Client on a removable medium (CD-ROM, DVD-ROM etc.). This service will be invoiced by the Company at a price of €285 ex. VAT per removable medium.

Retrieval by the Company shall release the latter from its obligation to store the Archives.

Should the Client fail to retrieve its Archives within the time-frame mentioned above, the Company shall destroy the relevant Archive set.

Article 9. SERVICE LEVELS

The Company implements all the necessary means to ensure the performance and optimal availability of the EDA Service.

The Company provides support relating to the use of the EDA Service in French and by email. The support service is only accessible to the single Application Administrator. The Client undertakes to provide the most accurate description of any issue encountered so that the Company may assess its cause and remedy the issue. Based on the description of the problem encountered by the Client, the Company will respond to any support request within a period of two (2) business days from receipt of the support request email.

The availability guarantees described below apply solely to the infrastructure and equipment which constitute the Company's Electronic Archive Centre (EAC) and enable the EDA Service to be provided to the Client.

This guarantee specifically excludes all the Client's equipment and infrastructure as well as the equipment and infrastructure lying between the Client and the Company's Electronic Archive Centre (EAC).

Given ongoing technological developments, the Company reserves the right to update its service levels at any time, after having notified the Client of the alterations made, provided the level of quality the service remains unaltered or is improved.

9.1 Average availability rate excluding maintenance and penalties

- The half-yearly average availability rate for the Upload function is 99.8%.
- The yearly average availability rate for the Upload function is 99.7 %.

9.2 Maintenance

In order to ensure optimal service and its full operation, the Company may need to interrupt the EDA Service for maintenance reasons.
For instance, service interruptions for ongoing maintenance should for the most part occur between 0:00 am (midnight) and 04:00 am (four) in the morning, and be limited to one per quarter.
The Client shall be notified by e-mail before any maintenance-related Service interruptions. To this end, the Client shall provide the Company with the name, telephone number and email address of the person who should be thus notified by the Company. The Client also agrees to immediately inform the Company of any change in the contact person or contact details, as appropriate. In addition, the Company declines all responsibility for late or missing notifications to the Client if the latter does not keep its files up to date.

Further, in the event of a technical alteration to the Service that would alter the way in which the Client uses the Upload or Consultation functions via the API, the Company shall inform the Client by any means necessary, with a 30 (thirty) day notification period.

Article 10. LIABILITY

As an Archive depository, the Company is obligated to fully retrieve all archived Electronic Documents on behalf of the Client; this is a performance requirement.

The Company shall be liable only for direct damages resulting from its own actions in the performance of its obligations, proof of which falls to the Client.

The Parties agree that the Company cannot be held liable, both with regard to the Client and to third parties, for any and all indirect damage such as business interruption, loss of customers, commercial harm, loss of investment, loss of data and/or files, loss of earnings, loss of opportunity or damage to the brand image, or for any incident and/or unavailability that may occur on the third party technical platform and the telecommunications networks used.

The Company has taken out a professional liability insurance policy covering non-material damage, consequential or otherwise, caused to the Client in the context of the performance of the EDA Service.

The Client acknowledges and accepts that the Reseller bears no liability to the Client with respect to the Company providing the EDA Service or any other service provided to the Client by the Company. The Client's sole recourse in the event of failure of the EDA Service or other services provided by the Company to a Client is limited to the Company. The Resellers waives all responsibility with respect to such failures.

Article 11. TERM-TERMINATION

The Company undertakes to maintain the Archives throughout the duration stipulated by the authorised Reseller.

Unless otherwise provided for, the Archive conservation period as offered by the authorised Reseller is 10 years per Archive. The Company expressly agrees to comply with this conservation period, regardless of any alteration made in the contractual agreements between the Parties.

The Client may, upon request and after the term of the Service, use a consultation service via the MyArkhineo portal for which it shall have 2 (two) accesses for Authorised Administrators. It shall be possible to increase the number of authorised accesses based on a quote drawn up in advance by the Company.

In the event of a serious breach by one Party of its obligations under this Agreement, that is not remedied within 30 (thirty) calendar days from receipt of a registered letter with acknowledgement of receipt notifying the breach in question, the other Party shall be entitled to terminate this Agreement, in whole or in part.

Regardless of the Contract termination circumstances, the Services provided to the Client by the Company at the effective termination date shall not be negated. Further, any amounts already invoiced for shall not be reimbursable and shall be due the Company.

Article 12. CONFIDENTIALITY

Information, data, and documents of any type that are transferred between the Parties as part of the Service shall be considered as Confidential Information. The Archives are the Client's Confidential Information and all of the documentation, know-how, methods, software as well as any technical, organisational or financial element are also considered the Company's Confidential Information.

However, information which: (i) was already in the public domain at the time of its disclosure to the receiving Party, and/or (ii) was known by the receiving Party, who can prove it, prior to its disclosure, and/or (iii) came into the public domain after its disclosure to the receiving Party, without that Party breaching the Agreement, and/or (iv) was sent to the receiving Party by a third party who was free to disclose it, shall not be considered Confidential Information.

Except in cases of legal disclosure obligations, namely to the Parties' auditors, the confidentiality obligation of this article extents to any duly authorised administrative or judicial authority, and the

obligation of disclosure must be brought to the attention of the other Party within a reasonable prior time-frame.

The confidentiality obligation stated in this article remains valid for a period of 3 (three) years following the termination of this contract for any reason whatsoever.

Article 13. PERSONAL DATA PROTECTION

It is agreed that the Reseller (Data Processor) shall use only sub-processor providing sufficient guarantees to implement appropriate technical and organisational measures to ensure its compliance with the applicable Data Protection laws.

The Data Processor shall enter into written agreement (DPA) with Docaposte Arkhineo by which it undertakes to comply with all applicable Data protection laws and obligations.

13.1 Notification :

In case of data protection violations as defined by the GDPR, Docaposte Arkhineo shall notify the Reseller 72 hours after becoming aware of the violation. On request, Docaposte Arkhineo shall provide the Reseller with a comprehensive, up to date data protection and security concept for the processing.

The notification shall be made to by e mail to security@docusign.com and shall contain the details necessary for reporting to the supervisory authorities.

13.2 Specific Audit

Upon Reseller's request, Docaposte Arkhineo will inform the Client as Data Controller of the measures it has taken to ensure compliance with its obligations under the data protection laws.

The Reseller reserves the right to audit or supervise Docaposte Arkhineo, directly or by a third party, at Reseller's costs, to ensure that Docaposte Arkhineo is compliant with data protection laws and obligations under this article.

13.3 Specific Provisions

The Company, in its capacity as subprocessor, undertakes the following:

- to take all required technical and organisational measures in accordance with any documented instruction that the Client, as the data controller, asks it to follow by express notification;
- not to use personal data for purposes other than those warranting the signature of these GTC;
- not to appoint another sub-contractor who may not provide sufficient guarantees as to the implementation of the appropriate technical and organisational measures and which has not been authorised, specifically or generally, in writing beforehand by the data controller;
- not to disclose personal data in any way or by any means, to staff members who are not expressly authorised to consult them by the Company or by the data processor, in accordance with these GTC and in accordance with any applicable laws and regulations;
- to take state-of-the-art security measures, namely and if required the anonymisation or encryption of personal data, and to implement any required mechanism to ensure the confidentiality, integrity, availability and resilience of processing systems, in order to prevent the fraudulent use of the data and maintain its integrity;
- to ensure that all staff who might have access to personal data shall comply with security and confidentiality requirements for said data, such employees consisting solely of authorised

personnel and, if applicable, that any further sub-contractors who may have access to personal data be required to comply with those same requirements;

- if applicable and at the express request of the data controller, on the basis of applicable rates, to facilitate the exercise by the data subjects – managing this itself – of their rights to access their personal data, and to correct or delete them as well as, in this context, to document complaints established by the data controller in this regard on the management system;
- not to transfer or allow any of its subsequent sub-contractors to transfer personal data outside the European Union without obtaining the Client's prior written authorisation;
- upon the expiry or termination of this Agreement, to destroy/return any personal data which might still be retained or archived by a sub-contractor, except for the period during which such archiving or retention is required by current laws or regulations, under the following terms and conditions. The Client acknowledges that the price of the services mentioned in this Agreement, as expressed in this Agreement, does not include the price and the costs related to the return of personal data;
- ensure that all requirements are complied with by any subsequent sub-contractor, regardless of their rank or the methods used to work on the services (including for maintenance purposes), that the sub-contractor may be called-upon to carry out, requiring by contract means and others that said sub-contractor explicitly comply with the obligations in the contract binding them to the subsequent sub-contractor in question and ensuring that that sub-contractor undertakes to comply fully with the obligations.

Given that the Client is fully responsible to comply with national or European laws and regulations with respect to the protection of Personal Data, the Client agrees to comply with all applicable laws and regulations. The Client acknowledges and accepts (in light of the current state of knowledge, implementation costs, the context and the purpose of the processing of personal data) that the security practices and strategies implemented by the Company guarantee an appropriate level of security for the risks to persons involved.

Article 14. Compliance with applicable anti bribery legislation

Docaposte Arkhineo undertakes to comply with the anti bribery laws applying in the regions (UE) in which is doing business.

Docaposte Arkhineo implemented a Code of Conduct which sets clear guidelines for all employees regarding the expected behaviors while exercising their roles and responsibilities.

Compliance with the Code of Conduct is enforced through internal policies and procedures. These policies, procedures and the corresponding trainings will help employees fulfill their roles and responsibilities with regard to the conduct guidelines.

Docaposte Arkhineo shall provide written certification to Reseller that employees have fully complete anti bribery training

Docaposte Arkhineo must ensure compliance with embargo measures issued mainly by France, the European Union, the United States and the United Nations for Docaposte Arkhineo's activities.

To fight criminal and terrorist activities, Docaposte Arkhineo is committed to complying with applicable laws and promoting a strong ethical and compliance culture.

Docaposte Arkhineo promote a behaviour in accordance with best practices with regard to environnemental and social responsibility.

Article 15. AUDIT

The Company undertakes to carry out a yearly audit at its own expense, using internal auditors or a recognised certification authority. This audit covers all the services provided to the Client under the EDA Service, and in particular those aspects that support the maintenance of the NF 461 certification.

In the event that an audit discovers a deviation from the certification standards, the Company shall take the necessary corrective measures at its own expense.

Article 16. APPLICABLE LAW

The Contract is governed by French law with respect to both its formal validity and its contents. ANY DISPUTE REGARDING THE VALIDITY, INTERPRETATION OR EXECUTION OF THE TERMS AND CONDITIONS SHALL BE SUBMITTED TO THE RELEVANT COURT IN PARIS, INCLUDING WHEN MULTIPLE DEFENDANTS OR THIRD-PARTIES ARE INVOLVED, EVEN IN PRELIMINARY PROCEEDINGS, ON A SUMMARY OR EX-PARTE BASIS.

Given the confidentiality requirements involved in Archiving and the fact that the Company is not able to carry out any checks on the content of the Documents received, the Client expressly states to the Company that all of its Archives shall comply with the laws and regulations applicable in France or in Europe, and that it has taken all measures required to protect personal privacy. Therefore, the Client guarantees the Company against any liability related to the content and use of the Archives.

Moreover, it is specified that the Company shall respond to any demand or request issued by a judicial or administrative authority with jurisdiction, within the framework of applicable laws.

Article 17. GENERAL PROVISIONS

- In the event that one of the clauses of this contract be deemed invalid or declared as such by a final ruling given by a court with jurisdiction, the other clauses shall remain valid and in effect.

- The fact that one of the Parties does not avail itself of a breach of contract by the other Party shall in no way be subsequently interpreted as a waiver of the requirement to comply with the obligation that was breached.

- The Client accepts that the Company may use its company name or one of its trademarks or logos, as a marketing support with regard to third parties.

- The Company may sub-contract all or part of its obligations to third parties, on the condition and with the exception of emergencies or cases of force majeure that it has obtained prior and express acceptance from the Client for each sub-contractor, and provided that the Company retains sole liability, with regard to the Client, for the proper performance of this contract.

As an exception, it is already specified that, for reasons of physical and IT security, the physical archiving centre used for the purposes of the Service is located within the computer infrastructures of the Caisse des Dépôts et Consignations.

It is agreed that the Company may freely sub-contract all or part of its obligations to an entity affiliated with the Caisse des Dépôts, as defined by Article L 233-3 of the French Commercial Code. The Client may not transfer its rights or obligations, in part or in whole, without having obtained the prior and

written approval of the Company. For the hosting of Personal Health Data, the Company undertakes that the assignee shall hold the “Personal Health Data Host” authorisation.

- No action of any kind arising from this contract may be undertaken by one of the Parties more than six (6) months after said Party has become aware of the triggering event justifying such an action.

- The Client and the Company agree that using an authentication method specific to each Authorised User is a valid and binding method of authentication. In particular, the Client acknowledges that the Company has legitimate grounds to consider any Upload as coming from an Authorised User and having the value of a document as defined in articles 1366 *et seq.* of the French Civil Code.