Appendix 4 – Data Processing Agreement

Provider will make available the Software to the Customer in accordance with the Agreement and will process personal data on behalf of Customer as a result thereof. This Data Processing Agreement (hereinafter the "**DPA**") sets out the terms and conditions between the Provider and the Customer for such processing of personal data.

1. DEFINITIONS

Terms used but not defined herein shall have the meanings set forth on the Cover Document and the General Terms and Conditions set forth in Appendix 2 to the Agreement. The following additional terms in this DPA shall have the following meaning:

"**Personal Data**"	means any information relating to an identified or identifiable natural person, which is Processed by Provider solely on behalf of Customer under the Agreement and this DPA;
"**Process**" or "**Processing**"	means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
"**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 of Personal Data.
"**Processor**"	means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller
"**Data Subject**"	means an identified or identifiable natural person to whom the Personal Data relates.
"**Sub-processor**"	means any third party that Processes Personal Data under the instructions of Provider.

viedoc™

Appendix 4 – Data Processing Agreement

2. PROCESSING OF PERSONAL DATA

2.1. For the avoidance of doubt, for any Personal Data Processed by Provider under this DPA, as between the Parties, Customer shall either be

a) the Controller of the Personal Data, or

b) the Processor to a third party which is the Controller of the Personal Data.

For this purpose, in situations set out in section 2.1(a), Provider shall be considered the Data Processor of Customer and in situations set out in section 2.1(b), Provider shall be considered the Sub-processor of Customer.

2.2. Provider undertakes to only Process Personal Data in accordance with documented instructions from the Customer, unless otherwise provided by applicable laws and regulations. The Customer's initial instructions to the Provider regarding the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects, and technical and organizational measures are set forth in this DPA and in Schedule A.

2.3. The Customer confirms that, except for any written instruction provided in specific cases according to clause 2.4, the obligations of Provider set out in this DPA, including Schedule A, constitutes the full and complete instructions to be carried out by Provider as Processor (or Sub-processor as the case may be). Any changes to the Customer's instructions shall be negotiated separately and, to be valid, documented in writing and duly signed by both parties. The Customer is required to not, without such written agreement, allow Provider to Process other categories of Personal Data, or to Process Personal Data about other categories of Data Subjects, or to Process Personal Data for other purposes than specified in Schedule A.

2.4. The Provider shall, to the extent required under applicable data protection laws and in accordance with the Customer's written instruction in each case, assist the Customer in fulfilling its legal obligations under such laws, including but not limited to the Customer's obligation to respond to requests for exercising the Data Subject's rights regarding Processing of their Personal Data.

2.5. The Provider shall immediately inform the Customer if, in its opinion, an instruction provided under this DPA infringes applicable data protection laws.

2.6. If Data Subjects, competent authorities or any other third parties request information from Provider regarding the Processing of Personal Data, Provider shall refer such request to the Customer without undue delay, unless prohibited under the law applicable to the requesting third party, and, if prohibited from notifying Customer, use all lawful

efforts to obtain the right to waive the prohibition in order to communicate as much information to Customer as soon as possible. Provider may not in any way act on behalf of or as a representative of the Customer and may not, without prior instructions from the Customer, transfer or in any other way disclose Personal Data or any other information relating to the Processing of Personal Data to any third party, unless otherwise required by applicable law or pursuant to a non-appealable decision by a competent court or authority.

2.7. In the event Provider, according to applicable laws and regulations, is required to disclose Personal Data that Provider processes on behalf of the Customer, Provider shall be obliged to inform the Customer thereof immediately, unless otherwise provided by applicable law or pursuant to a decision by a competent court or authority, and request confidentiality in conjunction with the disclosure of requested information.

3. SUB-PROCESSORS

3.1. In addition to Sub-processors listed in Schedule B, the Provider may engage additional or replacement Sub-processors without prior written consent from the Customer. The Provider shall ensure that Sub-processors are bound by written agreements that require them to comply with corresponding data Processing obligations to those contained in this DPA.

3.2. If the Provider intends to engage a new Sub-processor that will Process Personal Data covered by this DPA, the Provider shall, prior to such engagement, inform the Customer thereof. The Provider shall provide the Customer with any information reasonably requested by the Customer to enable the Customer to assess the use of the proposed Sub-processor against applicable laws and regulations.

3.3. The Provider is responsible for its Sub-processors and shall remain liable towards the Customer for any Sub-processor's acts and/or omissions.

4. TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES

4.1 Provider's Processing of Personal Data under this DPA will take place within the relevant geographical region as described in Schedule A, section 5, and as agreed in the relevant Work Order (hereinafter the "Processing Operations Region"). Provider makes the following commitment regarding transfers of Personal Data to third countries outside the Processing Operations Region:

a) Provider will not transfer any Personal Data outside the Processing Operations Region,

b) Provider will not instruct any Sub-processors to transfer any Personal Data outside the Processing Operations Region, and

c) Provider will ensure contractual arrangements are put in place with all Sub-processors that include

   a. restrictions on transfers of Personal Data outside the Processing Operations Region, unless such transfer is mandatory under applicable laws and regulations or subject to a legally binding request for disclosure of the Personal Data by a law enforcement authority, and

   b. obligations on the on Sub-processor to (i) inform the Provider of any disclosure request (if permitted by law to do so) and to redirect the request to the Provider (if permitted by law to do so), (ii) to assess the legality of a request and seek legal protection from any (disproportionate) disclosure request, (iii) only provide the minimum amount of information permissible in response to any disclosure request, and (iv) document and record the requests for access received from public authorities and the response provided, alongside the legal reasoning and the actors involved.

4.2 Provider cannot and do not monitor or control how the Customer distributes access rights to the Software within each Study, or from where each Software user accesses the Software. It is the Customer's sole responsibility to control user´s access to the Software within its Studies and to determine from where such access may take place, be it from within or outside the Processing Operations Region.

5. INFORMATION SECURITY AND CONFIDENTIALITY

5.1. Provider shall be obliged to take appropriate technical and organizational Measures to protect the Personal Data which is Processed. The measures shall result in a level of security which is appropriate taking into consideration:

a) existing technical possibilities;

b) the costs for carrying out the measures;

c) the particular risks associated with the Processing of Personal Data; and

d) the sensitivity of the Personal Data which is Processed.

5.2. Provider shall maintain adequate security for the Personal Data. Provider shall protect the Personal Data against destruction, modification, unlawful dissemination, accidental or unlawful access. The Personal Data shall also be protected against all other

forms of unauthorized Processing in violation of this DPA or applicable laws and regulations. Taking into account the state of the art and the costs of implementation and the nature, scope, context and purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, the technical and organizational measures to be implemented by Provider shall include, as appropriate:

a) the encryption of Personal Data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services Processing Personal Data;

c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

5.3. Provider shall notify the Customer of any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data or any other security incidents (hereinafter "Personal Data Breach") immediately upon becoming aware of such incidents. The notification should at least:

a) describe the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

c) describe the likely consequences of the Personal Data Breach; and

d) describe the measures taken by Provider or proposed to be taken by the Customer to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

5.4. In case of a Personal Data Breach, and taking into account the nature of Processing and the information available to the Provider, the Provider shall provide reasonable assistance to the Customer to help the Customer comply with it's obligations for (i) notification of a Personal Data Breach to the relevant supervisory authority, as applicable, and (ii) communication of a Personal Data Breach to the relevant Data Subjects, as applicable and appropriate.

5.5. The Provider undertakes not to, without the Customer's prior written consent disclose or otherwise make Personal Data Processed under this DPA available to any third party, except for Sub-processors engaged in accordance with this DPA, unless otherwise required under applicable laws and regulations or pursuant to a decision by a competent court or authority.

5.6. The Provider shall be obliged to ensure that only such staff as directly requires access to Personal Data in order to fulfil the Provider's obligations in accordance with this DPA have access to such information. The Provider shall ensure such staff is bound by a confidentiality obligation concerning this information to the same extent as the Provider in accordance with this DPA.

5.7. The duties of confidentiality set forth in this section 5 shall survive the expiry or termination of the DPA.

5.8. Provider shall, in addition to 5.1-5.6, take the technical and organizational security measures agreed between the Parties in Schedule A attached to this DPA to protect the Personal Data against accidental or unlawful destruction or accidental loss, damage, alteration, unauthorized disclosure, use or access and against all other unlawful forms of Processing.

6. AUDIT RIGHTS

a. The Customer shall be entitled to take measures necessary to verify that Provider is able to comply with its obligations under this DPA, and that Provider has in fact undertaken the measures to ensure such compliance. Provider undertakes to make available to the Customer all information and all assistance reasonably necessary to demonstrate compliance with the obligations laid down in this DPA and allow for and contribute to audits, including on-site inspections, conducted by the Customer or another auditor mandated by the Customer.

b. The Customer shall ensure that any designee third party carrying out the audit enters into a non-disclosure agreement and that such third party takes necessary security measures when conducting the audit.

c. If the audit shows that there are security deficiencies and such deficiencies are a result of the Provider's noncompliance with this DPA, the Provider shall bear the costs for the rectification of the deficiencies. If the audit shows that there are security deficiencies and such deficiencies are a result of inadequate instructions from the Customer, then the Provider and the Customer shall

discuss the nature of the problems the audit points out and shall decide how to rectify them and how to reasonably and fairly share the costs.

7. LIMITATIONS OF LIABILITY

7.1. The limitations of liability set out in section [12] of the General Terms and Conditions shall apply to Provider's liability under this DPA as if set out herein.

7.2. Provider shall only Process Personal Data in accordance with Customer's Instructions. Therefore, Provider is not liable in circumstances where Provider's actions result from instructions received from Customer.

8. TERM

8.1. This DPA shall enter into force when Cover Document is duly signed by each Party. The provisions in this DPA shall apply during such time that Provider Processes Personal Data on behalf of the Customer.

9. MEASURES UPON COMPLETION OF PROCESSING OF PERSONAL DATA

9.1. Upon expiry of this DPA, the Provider will, at Customer's discretion, erase or return all Personal Data processed under this DPA within thirty (30) days after the termination of the Cover Document, unless continued Processing of Personal Data is required under applicable laws and regulations.

9.2. Upon request by the Customer, Provider shall provide a written notice of the measures taken regarding the Personal Data upon the completion of the Processing.

10. LAW AND DISPUTES

10.1. The provisions on governing law and disputes in Section 18 of the General Terms and Conditions shall apply also to this DPA.

viedoc™

Appendix 4 – Data Processing Agreement

SCHEDULE A TO APPENDIX 4

DATA PROCESSING INSTRUCTIONS

1. Nature and Purposes

The Provider is a software vendor providing a platform with the purpose to collect and store research data according to a Study protocol in an auditable, secure and structured manner.

2. Categories of Data Subjects

The Personal Data processed will concern the following three types of Data Subjects:

A. Data Subjects who are participants in a Study conducted using the Software ("**Study Subjects**")

B. Software users (excluding Study Subjects using ViedocMe) in a Study conducted using the Software ("**Software users**")

C. Study staff captured in Trial Master File ("**TMF**") in the Software

3. Categories of Personal Data

The categories of Personal Data processed are, for Data Subject types A, B and C above, respectively:

A. Data points to be collected for the Study Subjects according to how the Study is configured ("**Study Configuration**")

B. Activity data of Study Subjects, when using ViedocMe, as part of the audit collection of the Study performance

C. Activity data of Software users as part of the audit collection of the Study performance

D. TMF data of Study Subjects, Software users and Study staff, such as Curriculum Vitae, logs, reports, agreements or financial information, as determined by the Customer

E. Contact details of Software users as part of authentication and the audit collection of the Study performance

F. Contact details of Study subjects, when using ViedocMe together with the Study subject reminder functionality

G. Video and audio streams between Study subjects and Software users when using ViedocConnect

4. Processing Operations

I. Category A and D data for Data Subjects A, B and C is added/edited/deleted by Data Subjects B having permission to do so according to Study Configuration decided by the Customer

II. Category B and C data for Data Subjects A and B is automatically added by the Software – this data cannot be edited but only deleted as part of a decommissioning Software function initiated by Data Subjects B having a special permission decided by the Customer

III. Category E data for Data Subjects B is added/edited/deleted by Data Subjects B

IV. Category F data for Data Subjects A is added/edited/deleted by Data Subjects B and can also be edited and deleted by the Study Subjects themselves, as applicable and in accordance with Study Configuration. This data is never decrypted for other purposes than for the system to be able to send the reminders. On the European instance, encryption and decryption keys are separated on different Sub-processors in different jurisdictions.

V. Categories A-F data is stored at primary data-center, disaster-recovery data-center and backup archive

VI. Categories A-F data is automatically processed as initiated by Data Subjects B, through and within the scope of Software functions allowed by the Customer as part of the Study Configuration – this includes but is not limited to listing, aggregating and transforming the data in various ways

VII. Category G data for Data Subjects A and B is automatically processed by the Software by live streaming during each ViedocConnect session. Data is never stored.

viedoc™

Appendix 4 – Data Processing Agreement

5. Location of Processing Operations

The table below sets out the country/region where each category of Processing activity takes place depending on the Software instance selected by the Customer. The Customer will decide upon the relevant instance for each specific Study, and this selection will be documented in the related work order.

Region / Data Processing	Europe instance	Japan instance	China instance
Primary data center	EU / EEA	Japan	China
Disaster recovery data center	EU / EEA	Japan	China
SMS and Email processing	EU / EEA	Japan and EU / EEA	China
Offline backup storage site	EU / EEA	Japan	China
Multi-party processing	EU / EEA	Japan	China
ViedocConnect live data stream	EU / EEA	EU / EEA	N/A

6. Technical and Organizational Measures (TOMs)

The Parties have agreed on the following technical and organizational measures:

Control type	**Purpose**	**Measures**	**Description of the respective solution**
Admission Control	Prevention of physical access to premises and facilities by unauthorized persons	Access control system, e.g. ID reader -, Smart card/transponder locking system.	All Provider data processing employ secure access processes, including Smart Card Readers.
		Surveillance facilities - Alarm system and camera recording of access	All Provider data processing employ secure access processes, including Surveillance facilities.

Appendix 4 – Data Processing Agreement

Control type	Purpose	Measures	Description of the respective solution
		Availability of Security staff, gatekeeper.	All Provider data processing employ secure access processes, including on-site security personnel.
		Employee identification badges/visibility of such.	All Provider data processing employ secure access processes, including provisioning and checking of employee identification badges.
		Control or monitor personnel (including third parties) who access secure areas.	All Provider data processing employ secure access processes, including control over who access secure areas.
		Physical hardware protection (e.g. door locking, lockable racks etc.).	All Provider data processing employ secure access processes, including physical hardware protection.
		Visual visitor control and guest lists at desk officer.	All Provider data processing employ secure access processes, including established visitor processes.
Insight Control	Prevention of use of data processing equipment by unauthorized persons by identification of use and control of authorization	Implementation of a central identity management system.	Provider leverages active directory as a central identity management system.
		Implementation of an enhanced user identification process (e.g. hardware token, biometric, etc.).	Two factors of authentication are required to access the Provider internal network – valid username/password combination and valid device certificate.
		Password procedures including frequency of their modification (e.g. length and complexity of password requirements, etc.).	Provider employs a strong password policy including password strength, complexity, and aging requirements.

viedoc™

Appendix 4 – Data Processing Agreement

Control type	Purpose	Measures	Description of the respective solution
		Automatic blocking or timeout of workstation and/or User ID after incorrect access attempts.	Provider locks user IDs after five unsuccessful logon attempts.
Access Control	Supplement to insight control; prevention of access of unauthorized persons to data to which they do not have access authorization	Differentiated access rights (profiles, roles, transactions and objects) to data and programs.	Provider employs, 'least privilege' for access to systems and data and elevated access rights are provided via a secondary account.
		Identification of accessing persons (e.g. no multi-user-accounts).	Unique user accounts are enforced and shared accounts are not permitted.
		Provide an enhanced user authentication process for remote system access from the Internet (e.g. 2-factor auth. using hardware token, etc.).	Two factors of authentication are required to access the Provider internal network – valid username/password combination and valid device certificate.
		Implement a concept for monitoring of information security and data protection.	Security event data sent to a centralized logging system for analysis and reporting.
		Automatic log-off in case of inactivity after defined time periods.	Password-protected screen saver enabled after 15 minutes of inactivity.
		Access to backup data and media is restricted.	Access to network backups restricted to authorized personnel only.
Transfer Control	Transfer of personal data and confidential business information via secure communication channels	Sending of email to external recipients only in encrypted form (PGP, TLS, etc.).	Opportunistic TLS enabled to email gateway.
		Use of digital signatures.	Digital signatures employed.
		Careful and regulated handling of portable storage media such as USB sticks, external hard drives, SD memory cards (e.g. encryption, storage in locked cabinets, etc.).	USB-write restrictions in-place in Provider. Only authorized users may write to portable devices and only approved portable devices

viedoc™

Appendix 4 – Data Processing Agreement

Control type	Purpose	Measures	Description of the respective solution
			(e.g. one containing encryption) may be used.
		Industry standard encryption of personal and confidential data when transferred through the internet (e.g. SFTP, https, VPN).	Provider required industry-standard encryption to be in place to protect all data exchanges over an unsecure network.
		Ensuring the establishment of an audit trail to document the transfer of personal and/or confidential data.	Records must be kept of data exchanges with third-parties.
Input Control	Traceability of new entries, modifications or deletions of personal data and confidential information (Audit Trail)	Ensuring the establishment of an audit trail to document whether and by whom personal data have been entered into, modified in, or removed from personal data processing systems (entry control).	Provider application has immutable audit-trail implemented according to industry standard
			Provider security events are logged and monitored using a SIEM system
		Protect log files against unauthorized use and modification.	Log files sent to centralized log collection server for analysis and storage. Access to centralized log collection server restricted to authorized personnel only.
		Implementation of a workflow to process sensitive data.	Provider has established change control and separation of duties processes in-place to protect sensitive data from unauthorized changes.
Order Control	Securing of transparency of actions of external contractors	Existence of formalized working instructions/procedures and appropriate training of employees and contractors.	Global information security awareness program deployed in Provider and is mandatory for all employees and contractors.

Appendix 4 – Data Processing Agreement

Control type	Purpose	Measures	Description of the respective solution
		Employees and contractors signed a written declaration to maintain confidentiality in accordance with the data protection law.	Employees/contractors must sign appropriate confidentiality agreements before granted access to the Provider network/ data assets.
Availability Control	Prevention of loss of personal data and other confidential information as well as the possibility for a reconstruction of data in case of loss with reasonable technical and organizational effort	Existence of tested and documented back-up and recovery concept.	Provider employs a network backup strategy of nightly, weekly, and monthly backups. Recovery efforts tested on a regular basis.
		Provide uninterruptible power supply (UPS).	Provider data centers contain robust power and HVAC controls included UPSes.
		Provide Air conditioning in server rooms.	Provider data centers contain robust power and HVAC controls including computer room air conditioning units (CRAC).
		Server rooms protected against fire, water and other physical damage.	Provider data centers contain robust power and HVAC controls including protections from fire, water, and other physical damage.
		Other measures.	Provider backs up data every 5 minutes using a geo-redundant backup solution Provider backups are transferred to a third location every 24 hours Provider performs restoration tests every 24 hours
Principle of adherence to intended purpose of data processing	Securing of exclusive use of personal data for the purpose for which it has originally been collected, separation of data collected for different purposes	Logical tenant separation (software-based).	Provider employs both logical and physical data segregation solutions.

viedoc™

Appendix 4 – Data Processing Agreement

Control type	Purpose	Measures	Description of the respective solution
		Separation of production and test system.	Provider employs DEV, TEST, UAT, and PROD environments.
		Roles and authorizations concept: administrator, reviser, user, etc.	Access to systems and data based on job role and need. Minimum amount of access needed to complete task is provided.
	Securing data minimisation, data quality and secure and relevant data retention and erasure	Measures for ensuring data minimisation	Provider application supports and promotes structured data collection according to a study protocol
		Measures for ensuring data quality	Provider application supports and promotes both manual and automated data quality review
		Measures for ensuring limited data retention	Provider application has self-service data-decommissioning features
			Measures for ensuring accountability
		Measures for allowing data portability and ensuring erasure	Provider application supports full data download in industry standard format (CDISC ODM) as well as generic formats (Excel, CSV, PDF)
			Provider application has self-service user removal features
Other Technical and Organizational Measures	Securing personal information in general and during transfer to third party country without an adequacy decision outside of the EU	Encryption of data in transit (i.e. transport encryption) using TLS 1.2 and AES 256-bit	Provider employs industry standard transfer mechanism of encrypted data for all transfers of personally identifiable information.
		Encryption of data at rest using 256-bit AES keys (CBC mode, PKCS5 padding, and random initialization vector).	

Appendix 4 – Data Processing Agreement

Control type	Purpose	Measures	Description of the respective solution
		Secure implementation of encryption, using tenant key management per platform with regular rotation.	
		Role-based restriction of access to personally identifiable information in relevant systems	
	Measures of pseudonymization of Study Subjects	Customer pseudonymizes Study Subjects using subject identification codes as customary in clinical trials	-
	Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Provider has an Information Security Management System implemented which is certified according to ISO 27001	-
	Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	Provider have implemented series of reviews, scans, evaluations to ensure this.	Provider have monthly access reviews implemented Provider perform monthly security vulnerability scans Provider perform monthly encryption-in-transit vulnerability evaluations Provider have implemented annual penetration tests by a third party Provider have implemented quarterly management review meetings
	Measures for ensuring system configuration, including default configuration	Provider hardens and validates all system configurations	Policies and SOPs describing relevant processes
	Measures for internal IT and IT security governance and management	Provider have implemented technical and organizational firewalls between Development and IT Operations	Provider employs strict separation between development and production operations departments, with documented handovers
	Measures for certification/assurance of processes and products	Provider has a Quality and Management System ("QMS") implemented	Within the QMS, Provider have implemented change management procedures
			Each Provider application updated is reviewed by QA department
			Risk Assessment is performed regularly including identification of gaps and mitigations
			Process for having available up-to-date policies and operational procedures

Appendix 4 – Data Processing Agreement

Control type	Purpose	Measures	Description of the respective solution
			Internal training of all employees, at onboarding and regular refreshers
			Continuous internal quality reviews and internal audits
			Due diligence in vendor selection

viedoc™

Appendix 4 – Data Processing Agreement

SCHEDULE B TO APPENDIX 4

VIEDOC RECORDS OF PROCESSING ACTIVITIES AND SUB-PROCESSOR LIST

Processor/ Sub-processor	Viedoc instance	Data location	Function(s) / categories of processing performed	ISO 27001	Supplemental measures	Data categories	Retention period	Contact information
Viedoc Technologies	**All**	**All**	**Processor responsible for all Sub-processor functions listed below**	**Yes**	**As per Schedule A**	**As per Schedule A**	**Per below**	dpo@viedoc.com or ciso@viedoc.com
Microsoft Azure China operated by 21Vianet	China	China	Infrastructure services	Yes	Encryption at rest, Encryption in transit, 2FA	All	Managed by Viedoc	Link, 21ViaNet, 12-13F, Building 6, No.6, Jiuxianqiao Road, Beijing Electronics Zone, Chaoyang District, Beijing, P.R. China, 100015
AliYun	China	China	Storage of encrypted backups without decryption keys, Email & SMS delivery	Yes	Encryption at rest, Encryption in transit, 2FA	All	Backup storage: Managed by Viedoc, Email & SMS: 30 days	Link
Amazon Web Services (AWS) operated by NWCD	China	China	Storage of encrypted backups without decryption keys	Yes	Encryption at rest, Encryption in transit, 2FA	All	Managed by Viedoc	Link, Ningxia Western Cloud Data Technology Co., Ltd., Room 201, Building A, Zhongguancun Park, Zhongwei Campus of Ningxia University, Shapotou District, Zhongwei City, P.R. China, 755000
Microsoft Azure Global	Europe	EU (France)	Infrastructure services	Yes	Encryption at rest, Encryption in transit, 2FA	All	Managed by Viedoc	Link, Microsoft EU Data Protection Officer, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland
OVH Cloud	Europe	EU (France)	Privacy data split-processing	Yes	Encryption in transit, 2FA	Email address, phone number & message content	No storage	Link, OVH SAS, Data Protection Officer, 2 rue Kellermann, 59100 Roubaix, France
Amazon Web Services	Europe	EU (Luxembourg, Ireland)	Storage of encrypted backups without decryption keys, Email & SMS delivery, Video/audio stream	Yes	Encryption at rest, Encryption in transit, 2FA	All	Backup storage: Managed by Viedoc, Email & SMS: 35 days, Video/audio stream meta-data: No storage	Link, Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855 Luxembourg

viedoc™

Appendix 4 – Data Processing Agreement

Processor/ Sub-processor	Viedoc instance	Data location	Function(s) / categories of processing performed	ISO 27001	Supplemental measures	Data categories	Retention period	Contact information
MailJet	Europe	EU (France, Germany, Belgium)	Email & SMS delivery	Yes	Encryption in transit	Email address, phone number & message content	6 days	Link, MailJet, 37B Rue Du Sentier, Paris, Ile-de-France, 75002, France
Elastic Email	Europe	EU (France)	Email & SMS delivery	No	Encryption in transit, 2FA	Email address, phone number & message contents	35 days	Link, Elastic Email, Attn: Privacy Officer, Unit 107, 1208 Wharf Street, Victoria, BC V8W 3B9, Canada
SMS Teknik	Europe	EU (Sweden)	SMS delivery	No	Encryption in transit, 2FA	Phone number & message contents	90 days	Link, SMS Teknik, Uddarne Industriväg 6, 45535 Munkedal, Sweden
WhereBy	Europe	EU (Luxembourg, Ireland)	Video/audio stream/UI	No	Encryption in transit, 2FA	Video/audio stream meta-data	No storage	Link, Whereby AS, Gate 1 no. 107, 6700 Måløy, Norway
Microsoft Azure Global	Japan	Japan	Infrastructure services	Yes	Encryption at rest, Encryption in transit, 2FA	All	Managed by Viedoc	Link, Microsoft EU Data Protection Officer, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland
Amazon Web Services	Japan	Japan, EU (Luxembourg, Ireland)	Storage of encrypted backups without decryption keys, Privacy data split-processing, Email & SMS delivery, video/audio streams	Yes	Encryption at rest, Encryption in transit, 2FA	All	Backup storage: Managed by Viedoc, Email & SMS: 35 days, Video/audio stream meta-data: No storage	Link, Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855 Luxembourg
HENNGE	Japan	Japan	Email delivery	Yes	Encryption in transit, 2FA	Email address & message content	40 days	Link, HENNGE株式会社, 個人情報管理担当宛て, 〒150-0036, 東京都渋谷区南平台町16番28号 Daiwa渋谷スクエア
Elastic Email	Japan	EU (France)	Email & SMS delivery	No	Encryption in transit, 2FA	Email address, phone number & message contents	35 days	Link, Elastic Email, Attn: Privacy Officer, Unit 107, 1208 Wharf Street, Victoria, BC V8W 3B9, Canada
SMS Teknik	Japan	EU (Sweden)	SMS delivery	No	Encryption in transit, 2FA	Phone number & message contents	90 days	Link, SMS Teknik, Uddarne Industriväg 6, 45535 Munkedal, Sweden
WhereBy	Japan	EU (Luxembourg, Ireland)	Video/audio stream and UI	No	Encryption in transit, 2FA	Video/audio streams	No storage	Link, Whereby AS, Gate 1 no. 107, 6700 Måløy, Norway