DATA PROTECTION AGREEMENT (“DPA”)

Customer shall make available to Sinch and Customer authorizes Sinch to process information including personal data for the provision of the Services under the Agreement (hereinafter “**Agreement**”). The parties have agreed to enter into this DPA to confirm the data protection provisions relating to their relationship and so as to meet the requirements of applicable Data Protection Legislation.

1. DEFINITIONS

1.1 For the purposes of this DPA:

"**Data Protection Legislation**" means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data by the Customer as Data Controller, including without limitation all binding (inter)national laws and other binding data protection or data security directives, laws, regulations and rulings valid at the given time including any guidance and codes of practices issued by the applicable supervisory authority;

“**Personal Data**” means any information relating to an identified or identifiable natural person ("**data subject**"); an identifiable 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, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

“**(Data) Processing**” means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

“**Special Categories of Personal Data**” means information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning a natural person's sex life or sexual orientation or any other special category of data as is indicated within the deviations in Appendix 2 *Deviations based on applicable National legislation* or in the Service Order or Service Specification;

“**Technical and organisational measures**” or TOMs means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access. This includes the agreed applicable security requirements and security instructions and their updates applicable at each time and described in Appendix 1 *Technical and organisational measures* to this DPA or in the Service Order or Service Specification;

The terms "**data controller**" and "**data processor**", shall have the meanings given to them under the GDPR.

1.2 Capitalized terms used and not defined in this DPA have the meanings given to such terms in the Agreement.

2. ROLE OF THE PARTIES

The Parties understand that for the provision of the Services a distinction is made between two types of processing of personal data: (i) the provision of the services (i.e. the database of call data records and the logs created and managed by Sinch on behalf and under the supervision of Customer) for which Sinch will act as a data processor and agrees to comply with the respective obligations set out in this DPA, and (ii) the transmission of messages (i.e. A2P SMS) by Sinch and other Service Providers for which Sinch will act as a data controller and agrees to comply with the respective obligations set out in clause 14.

3. SUBJECT MATTER, NATURE AND PURPOSE OF SINCH’S PROCESSING OF PERSONAL DATA

3.1 The subject matter, nature and purpose of the processing of personal data under this DPA is Sinch performance of the Services pursuant to the Agreement and as further instructed by the Customer in its use of the Services (“**Instructions**”), unless required to do so otherwise by Data Protection Legislation and/or Relevant Laws. In such case (and if, to the extent permitted by Data Protection Legislation and/or Relevant Laws.

3.2 Instructions of the Customer shall be in written form (including, but not limited to, email) or can be given through settings and use of Sinch's portal(s) and/or software. In exceptional cases, Instructions may be given orally by the Customer. Such oral Instructions will be confirmed by the authorized person of Customer in writing or per email (in text form).

4. DURATION

4.1 Sinch shall only collect or process personal data for the duration of the Agreement to the extent, and in such a manner, as is necessary for provision of the Services and in accordance with the Agreement and Data Protection Legislation applicable to Sinch in its role as data processor.

4.2 The processing of personal data will be carried out by Sinch after the Agreement necessary to fulfil the obligations in in this DPA or when necessary due to mandatory law unless otherwise agreed upon in writing.

5. TYPE OF PERSONAL DATA PROCESSED

The following Categories of personal data may be processed to deliver the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to the following categories of personal data:

- Contact information (company, email, phone, physical address)
- First and last name
- ID data
- Title
- Position
- Employer
- Connection data
- Localisation data
- Other data as is defined within the Agreement as agreed upon between parties.

6. TYPE OF DATA SUBJECTS

The Customer may submit personal data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to personal data relating to the following categories of data subjects:

- Customers, business partners and vendors of the Customer (who are natural persons)
- Employees of contact persons of the Customer's customers, business partners and vendors
- Employees, agents, advisors, freelancers of the Customer (who are natural persons)
- Customer's Service user including any user of the Services, which Customer permits using the Services

7. SUB-PROCESSORS

7.1 The Customer agrees that Sinch may engage Sinch Affiliate or third parties to process personal data in order to assist Sinch to deliver the Services on behalf of the Customer ("**Sub-processors**"). Sinch has or will enter into written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA to the extent applicable to the nature of the Services provided by such Sub-processor.

7.2 When required by law, Sinch shall conclude additional agreements (for example, but not limited to, Business Associates Agreements as is required by The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and/or The Health Information Technology for Economic and Clinical Health act ("HITECH")).

7.3 The current Sub-processors for the Services are set out at https://www.sinch.com/data-protection-agreement/sub-processors/ ("**Sub-processor List**") and the Customer agrees and approves that Sinch has engaged such Sub-processors to process personal data as set out in the list. The Customer may find at https://www.sinch.com/data-protection-agreement/sub-processors/ a mechanism to subscribe to notifications of new Sub-processors for each applicable Service, to which Customer shall subscribe, and if the Customer subscribes, Sinch shall provide notification of a new Sub-processor(s) before authorising any new Sub-processor(s) to process personal data in connection with the provision of the applicable Service.

7.4 Sinch shall notify the Customer, in accordance with the mechanism set out in clause 10.2, thirty (30) days' in advance of any intended changes concerning the addition or replacement of any Sub-processor during which period the Customer may raise objections to the Sub-processor's appointment. Any objections must be raised promptly (and in any event no later than fourteen (14) days following Sinch's notification of the intended changes). Should Sinch choose to retain the objected to Sub-processor, Sinch will notify the customer at least fourteen (14) days before authorising the Sub-processor to process personal data and then the Customer may immediately discontinue using the relevant portion of the Services and may terminate the relevant portion of the Services. Sinch will refund the Customer any prepaid fees covering the remainder of the term of such relevant portion of the Service following the effective date of termination and there will be no penalty on either party.

7.5 Sinch may replace a Subprocessor without advance notice where the reason for the change is outside of Sinch's reasonable control and prompt replacement is required for security or other urgent reasons, such as but not limited to (suspected) non-compliance of a Subprocessor with Data Protection Legislation or the DPA between Sinch and the Subprocessor. In this case, Sinch will inform the Data Controller of the replacement Subprocessor as soon as possible following its appointment. Section 7.4 applies accordingly.

7.6 for the avoidance of doubt, where any Sub-processor fails to fulfil its obligations under any sub-processing agreement or under applicable law Sinch will remain fully liable to the Customer for the fulfilment of its obligations under this DPA.

8. INTERNATIONAL TRANSFER

8.1 Whenever Sinch (or its sub-processors) processes personal data in other countries than the country in which the Sinch is established, Sinch will ensure an adequate level of protection for personal data by means of organisational, technical and contractual measures as is required by Data Protectional Legislation and this DPA.

8.2 Where (i) Personal Data of another Data Controller is processed internationally and such international processing requires an adequacy means under the laws of the country of the Data Controller and the required adequacy means can be met by entering into Standard Contractual Clauses, the the transfer is made pursuant to European Commission approved Standard Contractual Clauses for the transfer of Personal Data. Customer provides a power of attorney for Sinch to enter into any such European Commission approved standard contractual clauses with a Sub-processor approved as set out in clause 7 in the name and on behalf of the Customer, or where (ii) Personal Data of an EEA or Swiss based Data Controller is processed in a country outside the EEA, Switzerland and any country, organization or territory acknowledged by the European Union as safe country with an adequate level of data protection under art. 45 GDPR and no other lawful transfer mechanism such as Binding Corporate Rules (art. 47 GDPR) or Code of Conduct (art. 40 GDPR) is available.

8.3 In case that European Commission approved standard contractual clauses are concluded between Sinch and the Customer, the following applies until a competent Member State supervisory authority, or an EU or competent Member State court approves a different lawful transfer mechanism that would be applicable to the data transfers covered by the Standard Contractual Clauses (in case if such mechanism applies only to some of the data transfers, the following clauses will remain applicable for the transfers that cannot be covered by this new lawful transfer mechanism):

(i) Rights granted to data subjects under this DPA and the European Standard Contractual Clauses may be enforced by the data subject against Sinch irrespective of any restriction in Clauses 3 or 6 of the Standard Contractual Clauses. These rights are personal and may not be assigned to others. The data subject may only bring a claim under this DPA and the European Standard Contractual Clauses on an individual basis, and not part of a class, collective, group or representative action.

(ii) In addition to Clause 5(b) of the Standard Contractual Clauses, Sinch agrees that it, at the time of concluding this Agreement, has no reason to believe that the legislation applicable to it or its sub-processors, including in any country to which personal data is transferred either by itself or through a sub-processor, prevents it from fulfilling the instructions received from the customer and its obligations under the Standard Contractual Clauses and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Standard Contractual Clauses, it will notify the change to Customer as soon as it is aware, in which case Customer is entitled to suspend the transfer of data and/or terminate the contract.

(iii) For purpose of this section, lawful efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction:

- In case Sinch receives an order from any third party for compelled disclosure of any personal data that has been transferred under the Standard Contractual Clauses, Sinch will, where possible, redirect the third party to request data directly from Customer.

- In case Sinch receives an order from any third party for compelled disclosure of any personal data that has been transferred under the Standard Contractual Clauses, use all lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with the law of the European Union or applicable Member State law.

9. TECHNICAL AND ORGANISATIONAL MEASURES

Sinch has implemented and maintains appropriate technical and organizational measures to protect personal data processed against unauthorized or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure. Such measures are described in Appendix 1 *Technical and Organisational Measures.*

10. QUALITY ASSURANCES AND OTHER DUTIES OF SINCH

10.1 Sinch shall comply with the following requirements being:

- no processing of personal data except on instructions from the controller, unless required to do so by an authority;
- Implementation of data processing register
- Implement technical and organizational measures to ensure a level of data security appropriate to the level of risk presented by processing personal data;
- Cooperation with the data protection supervisory authority in performance of its tasks
- Notification of a personal data breach to the supervisory authority and the data subject;
- Carrying out a data protection impact assessment when necessary according to law and consult the supervisory authority prior to data processing where the data protection impact assessment indicates that the processing would result in a high risk in absence of measures taken by the controller to mitigate the risk.

and ensures in particular compliance with the following requirements:

a) Appoint a data protection officer, who performs his/her duties in compliance with Data Protection legislation. The data protection officer's contact details are available at Sinch web page. If Sinch contracting party is not established in the European Union, Sinch will appoint a responsible contact person in the European Union and/or a data protection officer in accordance with Data Protection Legislation.

b) Confidentiality in accordance with Data Protection legislation. Sinch entrusts only such employees with the data processing outlined in this contract who have been bound to confidentiality and have previously been familiarized with the data protection provisions relevant to their work. Sinch and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Customer, which includes the powers granted in this Amendment, unless required to do so by Data Protection Legislation.

c) At the Customer's cost and expense and taking into account the nature of the processing and the information available to Sinch, provide such information and assistance as the Customer may reasonably require and within the timescales reasonably specified by the Customer to assist the Customer to comply with its obligations under applicable Data Protection Legislation which may include assisting the Customer to:

   i) notify the Customer of any request Sinch receives for a data subject relating to personal data processed and notify the data subject to contact the Customer if it wants to use its rights;
   ii) comply with its security obligations;
   iii) discharge its obligations to respond to requests relating to the exercise of Data Subject rights including right of access, right to rectification, right to erasure ("right to be forgotten") right to restriction of processing (to the extent that personal data is not accessible to the Customer through the Services); carry out Data Protection Impact Assessment and audit Data Protection Impact Assessment compliance and consult with the supervisory authority;
   iv) following Data Protection Impact Assessment.

d) For purpose of this section, lawful efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction:

   i) Unless prohibited by applicable law or a legally binding request of law enforcement, Sinch shall promptly notify the Customer of any request by, any government official, data protection supervisory authority or law enforcement authority in respect of any personal data and, if prohibited from notifying Customer, Sinch will 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;

e) Sinch shall periodically monitor the internal processes and the TOMs to ensure that processing within Sinch

area of responsibility is in accordance with the requirements of Data Protection Legislation and the protection of the rights of the data subject.

11. AUDITS AND INSPECTIONS

11.1 In the event that the Customer, a Regulator or data protection authority requires additional information or an audit related to the Services, then, Sinch agrees to submit access to its data processing facilities, data files and documentation needed for processing personal data. Sinch agrees to provide reasonable cooperation to during such operations including providing all relevant information and access to all equipment, software, data, files, information systems, etc., used for the performance of Services, including processing of personal data.

11.2 The audit right as described within clause 11.1 will become applicable for the Customer, in case Sinch has not provided sufficient evidence of its compliance with the technical and organizational measures. Sufficient evidence includes providing either: (i) a certification as to compliance with ISO 27001 or other standards implemented by Sinch (scope as defined in the certificate); or (ii) an audit or attestation report of an independent third party. An audit as described within clause 11.1 shall be carried out at the Customer's cost and expense. An audit can be done by the Customer or any third party reasonably acceptable to the Sinch (which shall not include any third party auditors who are either a competitor of Sinch or not suitably qualified or independent)) to ascertain compliance with this DPA, subject to being given reasonable notice (30 days), compliance with Sinch's Technical and organisational measures and the auditor entering into a non-disclosure agreement directly with Sinch.

12. NOTIFICATION OF A DATA BREACH

12.1 In the event of Sinch aware of any breach of security that results in the accidental, unauthorised or unlawful destruction or unauthorised disclosure of or access to personal data Sinch shall, among other things:

a) Notify the Customer in writing immediately but not later than 72 hours after becoming aware of the personal data breach;

b) Assist the Customer with regard to the Customers obligation to provide information to the data subject and to provide the Customer with relevant information in this regard;

c) Support the Customer in consultations with data protection authority.

12.2 To the extent legally possible, Sinch may claim compensation for support services under this clause 12 which are not attributable to personal data breaches caused by Sinch.

13. DELETION OF PERSONAL DATA

13.1 Sinch is obliged to erase personal data as stipulated in the Agreement and in accordance with the Data Protection Legislation and/or Relevant Laws.

13.2 Customer has the right to request execution of the rights and obligations described in clause 13.1 during the duration of the entire DPA.

13.3 Statutory retention obligations or contractual obligations towards Service Providers of Sinch (for example but not limited to operators) remain unaffected by the above provisions. Documentation serving as evidence for an orderly data processing in accordance with the provisions of the DPA shall be retained by Sinch after termination of the DPA according to Data Protection Legislation and/or Relevant Laws.

14. SINCH'S OBLIGATIONS AS DATA CONTROLLER

In situations where Sinch will act as a data controller, it undertakes to comply with its obligations under applicable Data Protection Legislation in respect of any personal data processed under the SA. It shall process such personal data in connection with the transmission of messages, and to fulfil its associated obligations under the Agreement or as may be required by law, court order or any government or regulatory authority and in accordance with its privacy policy which is available at https://www.sinch.com/privacy-policy/ as amended from time to time, if necessary.

15. CUSTOMER'S OBLIGATIONS

The Customer shall comply at all times with Data Protection Legislation in relation to the processing of personal data in connection with the Agreement and the Services. The Customer shall inform Sinch in writing in case

additional legislation is applicable on the Processing of Personal Data other than the legislation of the country where the Customer is established.

16. LIMITATION OF LIABILITY

16.1 Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA whether in contract, tort or under any other theory of liability, is subject to the Limitation of Liability section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and this DPA.

16.2 Clause 16.1 shall not apply if the damage has been caused by the incorrect implementation of the commissioned service by the Customer or by an instruction given by the Customer. In such case, Customer will be liable for such damage.

17. MISCELLANEOUS

17.1 The DPA forms an integral part of the Agreement between Customer and Sinch. In case of conflict between the mandatory provisions in the European Standard Contractual Clauses and this DPA, the European Standard Contractual Clauses shall prevail. In case of other conflicts between other documents (including in case of conflict between the Agreement and this DPA), the DPA will prevail.

17.2 Should any provision of this DPA be or become invalid or contain a gap, the remaining provisions shall remain unaffected. Customer and Sinch undertake to replace the invalid provision with legally valid provisions which come the closest to the interest of the invalid provision respectively fills out the gap.

APPENDIX 1 to the data protection Agreement – Technical and Organisational Measures

Sinch shall implement the measures described in this appendix, provided that the measures directly or indirectly contribute or can contribute to the protection of personal data under the Agreement concluded between the Parties for the processing of data.

The Technical and Organizational measures that are implemented by Sinch are based on the state of the art, the implementations costs and the nature, scope, circumstances and purposes of the processing and the likelihood and severity of the risk to rights and freedoms of individuals hold true. The Technical and Organizational Measures are subject to technical progress and development. In this respect Sinch is permitted to implement alternative adequate measures. The level of security must align with industry security best practice and not less than, the measures set forth herein. All major changes are to be agreed with the Customer and documented.

The Technical and Organizational Measures as are included within this Appendix are measures that are applicable on the Service(s) provided by Sinch. If necessary, for the Service, Sinch may include further Technical and Organizational measures in the Service Order or Service Specification.

1 Risk management and Procedures for validation, review and evaluation

i. Sinch shall identify and evaluate security risks related to confidentiality, integrity and availability and based on such evaluation implement appropriate technical and organizational measures to ensure a level of security which is appropriate to the risk.

ii. Sinch shall have documented processes and routines for handling risks within its operations and when processing personal data on behalf of the Customer.

iii. Sinch shall periodically assess the risks related to information systems and processing, storing and transmitting information.

iv. Sinch shall identify and evaluate security risks related to confidentiality, integrity and availability and based on such evaluation implement appropriate technical and organizational measures to ensure a level of security which is appropriate to the risk of the specific personal data types and purposes being processed by Sinch, including inter alia as appropriate:

   a) The pseudonymization and encryption of personal data;
   b) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
   c) The ability to restore the availability and access to the Customer's Data in a timely manner in the event of a physical or technical incident;

v. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

vi. Sinch shall periodically assess the risks related to information systems and processing personal data (e.g. when storing and transmitting personal data).

vii. Sinch shall regularly monitor, review and audit Sub-processor's compliance with the Technical and Organizational Measures and Sinch shall, at the request of the Customer, provide the Customer with evidence regarding Sub-processor's compliance with the Technical and Organizational Measures.

viii. Sinch will work in accordance with the principles of data protection by design and by default and has to provide sufficient documentation of the implementation of data protection by design and by default

2 Organizational Measures

The internal organization of the processor shall meet the specific requirements of data protection.

A. Policies and Policy Management

i. Sinch shall have a defined and documented information security management system (ISMS) including an information security policy and procedures in place, which shall be approved by Sinch's management. They shall be published within Sinch´s organization and communicated to relevant Sinch Personnel.

ii. Sinch shall periodically review Sinch's policies and procedures concerning data protection and information security and update them if required to ensure their compliance with the Technical and Organizational Measures and the data protection agreement.

B. Organization of Data Protection and Information security

i. Sinch shall appoint at least one data protection officer who has appropriate competence and who functions as the main contact person for data protection. If required by law, Sinch shall appoint a data protection officer on a company level.

ii. Sinch shall have defined and documented security roles and responsibilities within its organization.

C. Organizational Requirements

i. Sinch shall ensure that Sinch personnel handles information in accordance with the level of confidentiality required under the DPA and that it has the written commitment of the employees to maintain confidentiality.

ii. Sinch shall ensure that relevant Sinch personnel is aware of the approved use (including use restrictions as the case may be) of information, facilities, and systems under the DPA.

iii. Sinch shall ensure that any Sinch personnel performing assignments under the DPA is trustworthy, meets established security criteria and has been, and during the term of the assignment will continue to be, subject to appropriate screening and background verification (if allowed by applicable law).

iv. Sinch shall ensure that Sinch personnel with security responsibilities is adequately trained to carry out security related duties.

v. Sinch shall provide or ensure periodical awareness training to relevant Sinch personnel. Such Sinch training shall include, without limitation:

a) How to handle customer information security (i.e. the protection of the confidentiality, integrity and availability of information);
b) Why information security is needed to protect customers information and systems;
c) The common types of security threats (such as identity theft, malware, hacking, information leakage and insider threat);
d) The importance of complying with information security policies and applying associated standards/procedures;
e) Personal responsibility for information security (such as protecting customer's privacy-related information and reporting actual and suspected data breaches).

3 Confidentiality

A. Access Control (Physical and environmental security)

i. Sinch shall protect information processing facilities against external and environmental threats and hazards, including power/cabling failures and other disruptions caused by failures in supporting utilities. This includes physical perimeter and access protection.
ii. Sinch shall protect goods from theft, manipulation, and destruction.
iii. Sinch shall specify authorized individuals allowed within its processing facilities and have an access control process.
iv. Additional measures for Data Centers:
a) All Data Centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Center facilities from being compromised.
b) Only authorized representatives have access to systems and infrastructure within the Data Center facilities.
c) To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.
d) Sinch and all third-party Data Center providers log the names and times of authorized personnel entering Sinch's private areas within the Data Centers.

B. Access control (Logical)

i. Sinch shall have a defined and documented access control policy for facilities, sites, network, system, application, and information/data access (including physical, logical and remote access controls), an authorization process for user access and privileges, procedures for revoking access rights and an acceptable use of access privileges for Sinch personnel in place.
ii. Sinch shall have a formal and documented user registration and de-registration process implemented to enable assignment of access rights.
iii. Sinch shall have a joiner-mover-leaver process for its employees.
iv. Sinch shall assign all access privileges based on the principle of need-to-know and principle of least privilege.
v. Sinch shall use strong authentication (multi-factor) for remote access users and users connecting from untrusted network.
vi. Sinch shall ensure that Sinch Personnel has a personal and unique identifier (user ID), and use an appropriate authentication technique, which confirms and ensures the identity of users.

C. Cryptography/Pseudonymization/Anonymization

i. Sinch shall ensure proper and effective use of cryptography on information classified as confidential and secret (such as personal data).
ii. Sinch shall protect cryptographic keys and store these in accordance with applicable legislation.

iii. Sinch will implement adequate measure for pseudonymization (substitution of personal identifiers with non- personal information) where appropriate.
iv. Sinch will implement adequate measure for anonymization (deidentify personal identifiers with non-personal information) where appropriate.

D. Guidelines concerning the admission to the Customer's premises and/or Sinch premises

Admission to the premises and property (such as datacenter buildings, office buildings, technical sites) is subject to the following:

i. Sinch shall follow local regulations (such as regulations for “restricted areas”) for the Customer’s premises when performing the assignments under the Agreement.
ii. Sinch Personnel shall carry ID card or, in case of visitors, a visitor’s badge visible at all time when working.
iii. After employment or completing the assignment, or when Sinch personnel is transferred to other tasks, personnel shall without delay inform authorized personnel of the change and return any keys, key cards, certificates, visitor's badges and similar items.
iv. Keys or key cards shall be personally signed for by Sinch personnel and shall be handled according to the written rules given upon receipt.
v. Loss of the key or key card shall be reported without delay to the authorized personnel.
vi. Photographing in or at the premises without permission is prohibited.
vii. Goods shall not be removed from the premises without permission.
viii. Sinch Personnel shall not allow unauthorized persons access to the premises.

4 Operations security

i. Sinch shall have an established change management system in place for making changes to business processes, information processing facilities and systems. The change management system shall include tests and reviews before changes are implemented, such as procedures to handle urgent changes, roll back procedures to recover from failed changes, logs that show, what has been changed, when and by whom.
ii. Sinch shall implement malware protection to ensure that any software used for Sinch’s provision of the Services to the Customer is protected from malware.
iii. The company network is protected from the public network by firewalls.
iv. Sinch shall make backup copies of critical information and test back-up copies to ensure that the information can be restored as agreed with the Customer.
v. Sinch shall log and monitor activities, such as create, reading, copying, amendment and deletion of processed data, as well as exceptions, faults and information security events and regularly review these. Furthermore, Sinch shall protect and store (for at least 6 months or such period/s set by Data Protection Legislation) log information, and on request, deliver monitoring data to the Customer. Anomalies / incidents / indicators of compromise shall be reported according to the data breach management requirements as set out below.
vi. Sinch shall manage vulnerabilities of all relevant technologies such as operating systems, databases, applications proactively and in a timely manner.
vii. Sinch shall establish security baselines (hardening) for all relevant technologies such as operating systems, databases, applications.
viii. Sinch shall ensure development is segregated from test and production environment.

5 Integrity

i. Sinch shall implement network security controls such as service level, firewalling and segregation to protect information systems.
ii. Sinch operates a phishing and SPAM detection system with the aim to protect its customers and Sinch (and the personal data of which these Parties are the Controller) against unwanted content and the spreading of SPAM/phishing and to comply with operator requirements and applicable legislation. The system retrieves the URL/s from the mobile terminated request message body and then enables URL validation by issuing a GET method request to the URL, and by expanding to the full URL as one would have it in the browser address bar. If necessary due to not sufficient information or a suspicion of non-compliant content, the entire page may be loaded and analyzed, including the content of such page. This is a machine learning algorithm (with human validation) that is designed to learn from confirmed phishing and SPAM detection and that data will be used for this purpose within the Sinch group. Sinch will not provide nor send personal data of which Customer is the controller to any third-parties outside the Sinch Group other than to subprocessors necessary to provide this functionality.
iii. Personal data being processed on behalf shall be processed solely in accordance with the Agreement and instructions of the controller to the processor.
iv. Sinch will work according to written instructions or agreements and documents belonging to that agreement.

6 Data breach management

i. Sinch shall have established procedures for data breach management.

ii. Sinch shall inform the Customer about any data breach (including but not limited to incidents in relation to the processing of personal data) as soon as possible but no later than within 72 hours after the data breach has been identified.
iii. All reporting of security related incidents shall be treated as confidential information and be encrypted, using industry standard encryption methods.
iv. The data breach report shall contain at least the following information:
  a) The nature of the data breach,
  b) The nature of the personal data affected,
  c) The categories and number of data subjects concerned,
  d) The number of personal data records concerned,
  e) Measures taken to address the data breach,
  f) The possible consequences and adverse effect of the data breach, and
  g) Any other information the Customer is required to report to the relevant regulator or data subject.

i. To the extent legally possible, Sinch may claim compensation for support services under this clause which are not attributable to failures on the part of Sinch

7 Business continuity management

i. Sinch shall identify business continuity risks and take necessary actions to control and mitigate such risks.
ii. Sinch shall have documented processes and routines for handling business continuity.
iii. Sinch shall ensure that information security is embedded into the business continuity plans.
iv. Sinch shall periodically assess the efficiency of its business continuity management, and compliance with availability requirements (if any).

8 System/software development and maintenance (when software development or system development is provided to the Customer by Sinch)

i. Sinch shall implement rules for development lifecycle of software and systems including change and review procedures.
ii. Sinch shall test security functionality during development in a controlled environment.
iii. Security patch management is implemented to provide regular and periodic deployment of relevant security updates.
iv. Sinch will work in accordance with the principles of data protection by design and by default and must provide sufficient documentation of the implementation of data protection by design and by default

Appendix 2 to the data protection Agreement – Deviations based on applicable National legislation

1. Spain

In case the Controller/Processor is situated in Spain, the technical and organizational measures to be taken by the Processor are subject to the Spanish data protection laws. In this case, the preamble of Appendix 1 of this DPA shall be complemented as follows:

"The Processor shall make sure that the following technical and organizational measures are in compliance with the "high level security" measures according to Spanish Royal Decree 1720/2007 Title VIII, Art. 80 ff. Processor shall implement in particular the requirements of section three (Art. 89 ff.) of Spanish Royal Decree 1720/2007, in case the requirements in this Appendix 1 are not in compliance with these requirements. In such case, Processor shall inform Controller and submit any amendments or deviations from this Appendix 1 it deems necessary for a prior approval by the Controller."

2. Canada

The definition "Special Categories of Personal Data" in Clause 1 of this DPA shall be amended as follows:

"**Special Categories of Personal Data**" shall mean information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life or any other personal that may be considered as sensitive data based on applicable legislation."

In addition to what is agreed upon in this DPA, the following is applicable concerning the transfer of Data:

"Controller acknowledges that Processor may transfer, store, and process Personal Data to territories outside of Canada, where it will be subject to the laws of the foreign jurisdictions in which it is held. Processor shall not, and shall make sure that any Affiliate or any third party with whom it contracts to Process Personal Data on its behalf in connection with the relevant Service(s) shall not:

- transfer Personal Data to a territory outside of Canada except on terms substantially similar to terms herein, which are agreed to prior to such transfer; or
- operate in relation to that Personal Data in any way which will put Controller in breach of its obligations under applicable privacy laws."

In addition to what is agreed upon in this DPA:

"Controller acknowledges that it possesses all necessary consents and legal authority from data subjects that would allow Processor to process the data."

In addition to what is agreed upon in Section 7 of this DPA:

"Parties will also cooperate with respect to any data breach notifications to Canadian regulatory authorities, individuals and other organizations that are required by law or otherwise advisable in the Controller's sole discretion."

Without limiting the terms and conditions of the DPA for Canada and the Agreement as far as it is applicable on Canada, the following apply:

"Processor will comply with all Canadian federal and provincial privacy and anti-spam legislation applicable to Controller and Processor in the course of processing any Data in connection with the Services, including all applicable notice, consent, content and unsubscribe requirements in connection with the sending of electronic messages and the installation of computer programs on another person's device.

Processor will provide that access to the Data is limited only to those employees and authorized agents of Processor who need to have access to the Data solely for the purposes of Processor rendering the Services."

3. Australia

Following the Australian Data Protection guidelines (Australian Privacy Principles; APP) from Schedule 1 of the "Privacy Amendment (Enhancing Privacy Protection) Act 2012", which is a Supplement to the "Privacy Act 1988", the following is applicable on the processing of personal data:

(i) "**Controller**" means a person who, alone or together with other persons, establishes the purposes and the manner of processing personal data; and "**Processor**" means any person (other than an employee of the Controller) who, on behalf of the Controller, personal data processes.

(ii) Where a Controller or its Authorized Users in Australia intend to collect Personal Data in the Cloud Service, the Controller undertakes to obtain the prior consent of each Data Subject to an International Transfer pursuant to this Schedule if and to the extent that is required according to the Privacy Act. The Controller hereby confirms that he has received the personal data and has informed the persons concerned about the disclosure of the personal data in accordance with the APP and the Privacy Act 1988. On this basis, the requirement of "Informed Consent" within 8.1 APP is deemed to have been met due to the exception of the "Informed Consent". Provided that the Informed Consent does not apply, this Schedule provides the framework for the protection of the personal data of the affected persons in Australia insofar as it provides at least essentially the same privacy

as the APP, and Processor and its sub-processors commit themself to a level of data protection which is the same level as set out in Sections 2, 3 and 6 of this schedule (exception of "Substantially Similar Law" under APP 8.2 (a)). With this, the in APP 8.1 stated requirement of "Substantially Similar Law" for this purpose is seen as fulfilled.

4. UK

Insofar as a Data Protection Act (including the new EU Data Protection Basic Regulation or its successor after Great Britain leaves the European Union) comes into force after the date of entry into force of this DPA and it is contrary to the terms of this DPA or otherwise requires an amendment to this DPA, a Party may notify the other party in order to start to negotiate the necessary amendments to this DPA in accordance with the principle of good faith.

5. Switzerland

In accordance with Art. 3 lit. b of the Swiss Federal Act of 19 June 1992 on Data Protection (FADP), the definitions in clause 1 of this DPA shall be amended as follows:

"**Data Subject**": natural or legal persons whose data is processed.

6. Italy

In accordance with Article 29 of the Italian Personal Data Protection Code states it is necessary to appoint the data processor conform Italian law and to describe the specific tasks that they have in accordance with the Italian Data Protection Code. By signing this DPA the Controller appoints the Processor as a Data Processor. The Data Processor shall process data in accordance with the regulations and safety measures provided by Legislative Decree no. 196/2003 and identified in Appendix B thereto "Technical specifications regarding minimum security measures" and the regulations and safety measures that will be provided as updates to those contained therein. The, to be taken, measures are described within this DPA and its Appendixes.

Specifically Data Processor agrees to perform his duties strictly in accordance with Instructions given to him by the Data Controller, and shall, pursuant to art. 29, paragraph 5 of Legislative Decree no. 196/2003, supervise the timely compliance of the tasks given to Data Processor.

The Data Processor undertakes to:

- provide the Data Processing services described in the DPA, particularly undertakes to complete any processing operation or set of operations, with or without the aid of electronic means, with respect to the collection, recording, organization, storage, consultation, processing, modification, selection, extraction, comparison, use, interconnection, blockage, communication, dissemination, cancellation and destruction of data, even if not registered in a database;
- perform the Services in accordance with the data protection requirements and only for the intended purposes as described in the DPA. The Data Processor is obliged to safeguard data secrecy according to Data Protection Legislation, particularly the Data Processor undertakes to complete the data processing operations referred to herein in a lawful and proper manner, that provides for maximum confidentiality and which will also provides for timely and full compliance with the applicable laws and regulations;
- apply measures that all personnel charged with handling data do so in compliance with current law and regulations, as well as any Instructions provided thereon;
- monitor that its processing of personal data complies with the requirements established by Legislative Decree no. 196/2003,
- store personal data collected in compliance with the security measures provide art. 31 et seq. of Legislative Decree 196/2003, ensuring the observance of minimum security measures.

Both, Controller and Processor acknowledge that the Technical and Organizational Measures of Appendix 1 of the DPA are currently sufficient to comply with the measures of art 31 et seq. of Legislative Decree 196/2003.
If necessary, a system administrator will be appointed within a separate Appointment letter for System administrator.

7. USA

The following definitions in clause 1 of this DPA shall be amended as follows:

"Personal data (in the USA the term Personally Identifiable Information is used): any individual element of information concerning the personal or material circumstances of an identified or identifiable individual;

Sensitive data (also known as "Special Categories of Personal Data"): information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life, social security number, driver's license number or state or federally issues identification card number, account number or credit or debit card number, or an account number in combination with any required security code, access code, or password that would permit access to an individual's financial account, or any other information the unauthorized disclosure of which may require Controller to notify affected individuals."

8. Singapore

In the case the Controller is situated in Singapore, the following text will be added to clause 4 of this DPA:

"The Processor will comply in a timely manner with the directions or decisions of any competent data protection and privacy authority in relation to the Data. The Processor will give the Controller such co-operation, assistance and information as the Controller reasonably requests to comply with its obligations under Data Protection Legislation."

9. Malaysia

In the case the Controller is situated in Malaysia, the definition of Special Categories of data ("Special Categories of Personal Data" shall mean information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life) in clause 1 of this DPA (Definitions) will be replaced with the following: "Special Categories of Personal Data" shall mean information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, the commission or alleged commission of any offence, physical or mental health or sex life.

In the case the Controller is situated in Malaysia, the following text of clause 8 of this DPA will be supplemented with "The Processor will implement the technical and organizational measures as specified in Data Protection Legislation and in Appendix 1 to protect the Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, use or access and against all other unlawful forms of processing".

In the case the Controller is situated in Malaysia, the following text will be added to clause 9.1(b) of this DPA:

"Both Parties agree to observe secrecy regarding any information acquired within the framework of the Agreement and this DPA, especially regarding the Data, taking into account the Controller's secret. This obligation continues to apply after termination of the DPA."

In the case the Controller is situated in Malaysia, the following text will be added to clause11of this DPA "The report will cover the objectives of the technical and organizational measures set out in Appendix 1 and Data Protection Legislation."

10. India

The following definitions in clause 1 of this DPA shall be amended as follows:

"**Personal Data**" means any individual element of information concerning the personal or material circumstances of an identified or identifiable individual. Personal information which is any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

"**Special Categories of Personal Data**" shall mean Sensitive personal data or information of a person; this means such personal information which consists of information relating to;—(i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details ; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise: provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

The following text will be added to clause 8 of this DPA:

"The Processor shall comply with the reasonable security practices and procedures prescribed by the Controller and/or the privacy policy of the Controller shall constitute reasonable security practices and procedures under section 43A of the (Indian) Information Technology Act 2000 and the rules issued by the Indian Government under such provision shall accordingly not be applicable."

11. China

The following text will be added to clause 16 of this DPA:

"Legal liability according to the laws of the People's Republic of China may apply depending on the agreements of the Controller with its customer."

12. Brasil

The following definitions set forth by clause 1 of this DPA shall be amended as follows:

"**Special Categories of Personal Data**" shall mean Sensitive personal data: this means such data concerning racial or ethnic origin, religious beliefs, political opinions, membership to a trade union or religious, philosophical or political organizations, data concerning health or a natural person's sex life, genetic or biometric data, when related to a natural person.

"**Data Processing"** shall mean any operation carried out with personal data, such as those that refer to the collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, information evaluation or control, modification, communication, transfer, diffusion or extraction.

In the case the Subprocessors are situated in Brazil, the obligations set forth by clauses 7.2, 7.4 and 7.5 of this DPA will not be applicable.

13. Colombia

In addition to what is agreed upon in clause 8 and 15 of this DPA, the following is applicable concerning the processing and transfer of Personal Data:
“Controller acknowledges that Processor may transfer, store, and process Personal Data to territories outside of Colombia, where it will be subject to the laws of the foreign jurisdictions in which it is held. Controller acknowledges that it possesses all necessary consents and legal authority from data subjects and registrations of databases that would allow Processor to process the data within databases and in countries that meet at least the same data protection standards (adequate level of protection) as the ones provided under Colombian laws (such as, but not limited to, Decree N° 90 of 2018, the Unique Circular from the Superintendence of Industry and Commerce and the External Circular Nº 005 of 2017 from the Superintendence of Industry and Commerce).

14. Argentina

In addition to what is agreed upon in clause 8 and 15 of this DPA, Parties agree to conclude the following Argentinian Standard Contractual Clauses for international transfer in case the Controller of the personal data is from Argentina and/or applicable Data Protection Legislation and/or the Argentinian Data Protection Authority require these clauses to be concluded:

Contrato modelo de transferencia internacional de datos personales con motivo de prestación de servicios

Entre, por una parte, _____, con domicilio en la calle_____, localidad_____, provincia de _____, Argentina, (en adelante, “el exportador de datos”) y, por la otra, _____ (nombre), _____ (dirección y país), (“en adelante, el importador de datos”), en conjunto “las partes”, convienen el presente contrato de transferencia internacional de datos personales para la prestación de servicios, sometiéndola a los términos y condiciones que se detallan a continuación.