Sign In App ®

Data Processing Agreement ("DPA")

This DPA forms part of the Agreement entered into between Sign In App ("**SIA**") and you (the "**Customer**") on the Effective Date (as defined in the Agreement). "**Sign In App**" has the meaning given at https://www.signincentralrecord.com/legal/contracting-entity and "**we**" or "**us**" means Sign In App. , and all references to the Agreement shall include this DPA (including the Standard Contractual Clauses, as defined below).

All capitalised terms not defined in this DPA shall have the meanings set forth in the Agreement. This DPA applies where, and only to the extent that, SIA processes your Personal Data that is protected by Data Protection Laws applicable to the EEA and the United Kingdom.

If the processing of your Personal Data involves an International Transfer, the EU Standard Contractual Clauses and/or the UK Standard Contractual Clauses (together, the "**Standard Contractual Clauses**"), as the case may be, and as stated in section 5, apply, and are incorporated by reference.

All capitalised terms not defined in this DPA shall have the meanings set forth in the Agreement.

Definitions

"Agreement"	means the written or electronic agreement between the Customer and SIA for the provision of Products and/or services by SIA to the Customer.
"**Customer Personal Data**"	means any personal data that SIA processes on behalf of the Customer as a processor pursuant to the Agreement, and as more particularly described in this DPA.
"**Data Protection Laws**"	means all data protection and privacy laws applicable to the processing of personal data under the Agreement, including, where applicable, EEA Data Protection Law and UK GDPR.
"**EEA Data Protection Law**"	means (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**"); and (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.
"**EEA**"	means, for the purposes of this DPA, the European Economic Area, namely the European Union Member States, Iceland, Liechtenstein and Norway.
"**EU Standard Contractual Clauses**"	means the new standard contractual clauses for processors as approved by the European Commission following the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 pursuant to Regulation (EU) 2016/679).
"**Security Incident**"	means any unauthorised or unlawful breach of security that leads to the accidental or unlawful destruction, loss, or alteration of, or unauthorised disclosure of or access to, Customer Personal Data on systems managed or otherwise controlled by SIA.
"**Sensitive Data**"	means (a) social security number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card); (c) employment, financial, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, or information about sexual life or sexual orientation; (e)

	account passwords; or (f) other information that falls within the definition of "special categories of data" under the UK GDPR or any other applicable Data Protection Laws.
"**Sub-processor**"	means any processor engaged by SIA or its Affiliates to assist in fulfilling its obligations under the Agreement or this DPA. Sub-processors may include third parties or Affiliates of SIA but shall exclude SIA employees or consultants.
"Third Country Sub-processor"	means any Sub-processor incorporated outside the EEA or UK and outside any country for which the European Commission or the UK Information Commissioner's Office (as applicable) has published an adequacy decision.
"**UK GDPR**"	means Regulation (EU) 2016/679 General Data Protection Regulation as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations, the Data Protection Act 2018 (and regulations made thereunder); and the Privacy and Electronic Communications Regulations 2003, in each case, as may be amended, superseded or replaced.
"UK Standard Contractual Clauses"	means either: (i) UK Data Transfer Addendum: the applicable EU Standard Contractual Clauses as amended by a data transfer addendum in a form adopted by the UK Information Commissioner's Office, as amended, superseded or replaced from time to time; or (ii) UK Controller- Processor SCC: an international data transfer agreement (IDTA) in the form published by the UK Information Commissioner's Office between a Controller as "data exporter" and a Processor as "data importer", as amended, superseded or replaced from time to time; or (iii) UK Controller-Controller Standard Contractual Clauses: a data transfer agreement in the form published by the UK Information Commissioner's Office between a Controller as "data exporter" and a Controller as "data importer", as amended, superseded or replaced from time to time.
The terms "personal data", "controller", "processor" "processing" and "Data Subject" shall have the meaning given to them in the UK GDPR, and "process", "processes" and "processed" shall be interpreted accordingly. A reference in this DPA to a "Section" means reference to the Sections of this DPA.	

1. Roles and Responsibilities

1.1 **Parties' roles.** As between SIA and the Customer, the Customer is the controller of Customer Personal Data, and SIA shall process Customer Personal Data only as a processor acting on behalf of Customer as described in Annex A (Details of Processing) of this DPA.

1.2 **Purpose limitation.** SIA shall process Customer Personal Data only in connection with the arrangements envisaged under this DPA and in accordance with Customer's documented lawful instructions, except where otherwise required by applicable law. Customer instructs SIA and its Sub-processors to process Customer Personal Data as reasonably necessary for the provision of the services contemplated by the Agreement and to perform its obligations under the Agreement.

1.3 **Sensitive Data**. The Customer is responsible for ensuring that suitable safeguards are in place prior to transmitting or processing, or prior to permitting Customer's Uses to transmit or process, any Sensitive Data via the Products.

1.4 **Customer compliance.** Customer represents and warrants, and shall procure that Users to whom the Customer Personal Data relates represent and warrant that (i) it has complied, and will continue to comply, with all applicable Data Protection Laws in respect of its processing of Customer Personal Data and any processing instructions it issues to SIA; and (ii) it has provided, and will continue to provide, all notice and has obtained, and will continue to obtain, all consents and rights necessary under Data Protection Laws for SIA to process Customer Personal Data for the purposes described in the Agreement. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired Customer Personal Data. Without prejudice to the generality of the foregoing, Customer agrees that it shall be responsible for complying with all laws (including Data Protection Laws) applicable to any emails or other content created, sent or managed pursuant to the Agreement, including those relating to obtaining consents (where required) to send emails, the content of the emails and its email deployment practices. SIA shall have no liability towards the Users, and the Customer shall fully indemnify SIA against all losses arising as a result of a User bringing an independent claim against SIA or its Affiliates under or in connection with this DPA.

1.5 **Notification obligations regarding the Customer's instructions.** SIA shall promptly notify the Customer in writing without any obligation to provide legal advice, unless prohibited from doing so under Data Protection Laws, if it becomes aware or believes that any data processing instruction from the Customer violates Data Protection Laws.

2. Sub-processing

2.1 **Authorised Sub-processors.** The Customer agrees that SIA may engage Sub-processors to process Customer Personal Data on the Customer's behalf. The Sub-processors currently engaged by SIA and authorised by Customer as identified here (https://www.signincentralrecord.com/legal/subprocessors). The Customer further agrees that SIA may transfer Personal Data to its Affiliates (as such term is defined in the Agreement) solely for the purposes of utilising shared business functions (e.g. accounting) and for group business performance analysis and always provided that any such transfer is made in accordance with a written data sharing agreement and in compliance with the Data Protection Laws.

2.2 **Objection to Sub-processors**. The Customer may object in writing to SIA's appointment of a new Sub-processor within seven (7) calendar days of receiving notice in accordance with Section 2.1, by email to the main portal user and to the tech portal contact, provided that such objection is based on reasonable grounds relating to data protection. If the Customer does not object to the Sub-processor within seven calendar days of receiving the information, the Customer shall be deemed to have accepted the Sub-processor. If the Customer has raised a reasonable objection to the new Sub-processor, and the parties have failed to agree on a solution within reasonable time, the Customer shall have the right to terminate the Agreement with a notice period determined by the Customer, without prejudice to any other remedies available under law or contract.

2.3 **Sub-processor obligations.** SIA shall: (i) enter into a written agreement with each Sub-processor containing data protection obligations that provide equivalent protection for Customer Personal Data as those in this DPA, to the extent applicable to the nature of the services provided by such Sub-processor; and (ii) remain responsible for such Sub-processor's compliance with the obligations of this DPA and for any acts or

omissions of such Sub-processor that cause SIA to breach any of its obligations under this DPA.

3. Security

3.1 **Security Measures.** SIA shall implement and maintain appropriate technical and organisational security measures to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of Customer Personal Data in accordance with SIA's security standards described in Annex B ("**Security Measures**"). The Customer acknowledges and agrees that the Security Measures which are to be implemented by SIA are appropriate to meet the requirements under applicable Data Protection Laws.

3.2 **Confidentiality of processing.** SIA shall ensure that any person who is authorised by SIA to process Customer Personal Data (including its staff, agents and subcontractors) shall be under an obligation of confidentiality commensurate with the obligations of confidentiality in the Agreement.

3.3 **Updates to Security Measures.** The Customer is responsible for reviewing the information made available by SIA relating to data security and making an independent determination as to whether the Licensed Software meets the Customer's requirements and legal obligations under the Data Protection Laws. The Customer acknowledges that the Security Measures are subject to technical progress and development and that SIA may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services provided to the Customer.

3.4 **Security Incident response.** Upon becoming aware of a Security Incident, a Party shall: (i) notify the other Party without undue delay after becoming aware of the Security Incident; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by the other Party; and (iii) promptly take reasonable steps to contain and investigate any Security Incident. Notification of or response to a Security Incident under this Section 3.4 shall not be construed as an acknowledgment by such Party of any fault or liability with respect to the Security Incident.

4. Security Reports

4.1 **Records.** Upon reasonable written request from the Customer, SIA shall make available to the Customer all information reasonably necessary to demonstrate compliance with this DPA, provided nothing in this Section 4.1 requires SIA to provide the Customer with any of SIA's Confidential Information.

5. International Transfers

5.1 **Limitations on International Transfer**. Personal Data from EEA, UK, or Swiss Data Controller(s) may only be exported to or accessed by SIA (or its Affiliates) or its authorised Sub-processors outside the EEA, the UK, or Switzerland, as applicable ("**International Transfer**"):

5.1.1 If the recipient, or the country or territory in which it processes or accesses Customer Personal Data, ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Customer Personal Data as determined by the European Commission or another regulatory body of competent jurisdiction; or

5.1.2 In accordance with the Standard Contractual Clauses and Multi-tier Framework as set out in Section 5.2 below.

5.2 The Standard Contractual Clauses apply where (i) there is an International Transfer to a country that does not ensure an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Customer Personal Data as

determined by the European Commission or another regulatory body of competent jurisdiction, and/or (ii) there is an International Transfer to a recipient that is not covered by an appropriate safeguard, including, but not limited to, binding corporate rules, an approved industry code of conduct, and individual adequacy decision by a regulatory body of competent jurisdictions, or an individual transfer authorisation granted by a regulatory body of competent jurisdiction.

5.3 **EEA Data transfers.** Where the Standard Contractual Clauses apply: (i) SIA agrees that it is the "data importer" and the Customer is the "data exporter" under the Standard Contractual Clauses; (ii) Annex A and Annex B of this DPA shall replace Annexes 1 and 2 of the Standard Contractual Clauses, respectively.

5.4 For Third Country Sub-processors, SIA shall ensure that such sub-processor has entered into the unchanged version of the Standard Contractual Clauses prior to the Sub-processor's processing of Customer Personal Data.

5.5 The Data Processor shall, upon written request of the Data Controller prior to transferring Customer Personal Data to Third Country Sub-processors, request the data importer to provide the Data Controller with a written assessment as to whether the law of the third country of destination ensures adequate protection, under Applicable Data Protection Law, of personal data transferred pursuant to the Standard Contractual Clauses, by providing, where necessary, additional safeguards to those offered by those Standard Contractual Clauses.

5.6 Furthermore, prior to transferring Customer Personal Data to Third Country Sub-processors or processing Customer Personal Data in such third countries, Data Processor must use best efforts to implement appropriate (in particular, but not limited to technical and organisational) guarantees capable of ensuring that data subjects whose personal data are transferred to the third country of destination pursuant to the Standard Contractual Clauses enjoy a level of protection essentially equivalent to that which is guaranteed under Data Protection Laws and Regulations.

6. Return or Deletion of Data

6.1 **Deletion on termination.** Upon termination or expiration of the Agreement, SIA shall (at the Customer's election) delete or return to the Customer all Customer Personal Data (including copies) in its possession or control, except that this requirement shall not apply to the extent SIA is required by applicable law to retain some or all of the Customer Personal Data, or Customer Personal Data it has archived on back-up systems, which SIA shall securely isolate, protect from any further processing and eventually delete in accordance with SIA's data retention policies, except to the extent required by applicable law.

7. Data Subject Rights and Cooperation

7.1 **Data subject requests.** SIA shall provide reasonable cooperation to assist the Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Customer Personal Data under the Agreement. In the event that any such request is made to SIA directly, SIA shall not respond to such communication directly except as appropriate (for example, to direct the data subject to contact the Customer) or legally required, without the Customer's prior authorisation. If SIA is required to respond to such a request, SIA shall promptly notify the Customer and provide the Customer with a copy of the request unless SIA is legally prohibited from doing so. For the avoidance of doubt, nothing in the Agreement (including this DPA) shall restrict or prevent SIA from responding to any data subject or data protection authority requests in relation to personal data for which SIA is a controller.

7.2 **Data protection impact assessment.** To the extent required under applicable Data Protection Laws, SIA shall (at the Customer's expense) provide all reasonably requested information regarding the Licensed Software or other products or services (as

applicable) to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

8. Audit Rights

8.1 Subject to this section 8, SIA shall make available to the Customer on request all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by the Customer or an auditor mandated by the Customer in relation to the Processing of the Customer Personal Data by SIA or authorised sub-processors.

8.2 Information and audit rights of the Customer only arise under section 8.1 to the extent that the DPA does not otherwise give the Customer information and audit rights meeting the relevant requirements of Data Protection Law.

9. Limitation of Liability

9.1 The Customer shall be liable for, and shall indemnify (and keep indemnified) SIA in respect of any and all action, proceeding, liability, cost, claim, loss, expense (including reasonable legal fees and payments on a solicitor and client basis), or demand suffered or incurred by, awarded against, or agreed to be paid by, SIA arising directly or in connection with Customer's processing activities that are subject to this DPA:

a) any non-compliance by the Customer with the Data Protection Laws;

b) any processing carried out by SIA in accordance with instructions given by the Customer that infringe the Data Protection Laws; or

c) any breach by the Customer of its obligations under the Agreement;

except to the extent that SIA is liable under Section 9.3.

9.2 SIA shall be liable for, and shall indemnify (and keep indemnified) the Customer in respect of any and all action, proceeding, liability, cost, claim, loss, expense (including reasonable legal fees and payments on a solicitor and client basis), or demand suffered or incurred by, awarded against, or agreed to be paid by, the Customer arising directly or in connection with SIA's processing activities that are subject to this DPA.

a) only to the extent that the same results from SIA's breach of, or non-compliance with, this Agreement, the Customer's instructions, or the Data Protection Laws; and

b) not to the extent that the same is, or are contributed to, by any breach of the DPA by the Customer.

9.3 The Customer shall not be entitled to claim back from SIA any sums paid in compensation by the Customer in respect of any damage to the extent that the Customer is liable to indemnify SIA under Section 9.2.

9.4 Any claims against SIA or its Affiliates under or in connection with this DPA (including, where applicable, the SCCs) shall be brought solely against the entity that is a party to the Agreement.

9.5 In no event shall any Party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

10. Relationship with the Agreement

10.1 This DPA shall remain in effect for as long as SIA carries out Customer Personal Data processing operations on behalf of the Customer or until termination of the Agreement (and all Customer Personal Data has been returned or deleted in accordance with Section 6.1).

10.2 The Parties agree that this DPA shall replace any existing data processing agreement or similar document that the Parties may have previously entered into in connection with the Agreement.

10.3 In the event of any conflict or inconsistency between this DPA and the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (a) Standard Contractual Clauses; then (b) this DPA; and then (c) the Agreement.

10.4 No one other than a party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.

10.5 This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

Annex A

Details of Data Processing

1. **Subject matter**: The subject matter of the data processing under this DPA is the Customer Personal Data.

2. **Duration**: As between SIA and Customer, the duration of the data processing under this DPA is until the expiration or termination of the Agreement in accordance with its terms.

3. **Purpose**: SIA shall only process Customer Personal Data for the following purposes: (i) processing to perform its obligations under the Agreement; and (ii) processing to comply with any other reasonable instructions provided by Customer (e.g., via email or support tickets) that are consistent with the terms of the Agreement (individually and collectively, the "**Purpose**").

4. **Nature of the processing**: SIA provides support to the Customer in their use of the Licensed Software as more particularly described in the Agreement.

5. **Categories of data subjects**: Customer's employees and Users (as such term is defined in the Agreement)

6. **Types of Customer Personal Data**: Customer may upload, submit or otherwise provide certain personal data to SIA, the extent of which is typically determined and controlled by Customer in its sole discretion, and may include the following types of personal data: Customer employees and Users: Identification and contact data (name, job title, contact details, including email address) and IT information (IP addresses, usage data, cookies data, online navigation data, location data, browser data) and, subject to Clause 2.3 of this DPA, Sensitive Data.

7. **Processing Operations**: Customer Personal Data will be processed in accordance with the Agreement (including this DPA) and may be subject to the following processing activities: Storage and other processing necessary to provide, maintain and improve the Products and Professional Services provided to Customer pursuant to the Agreement; and/or Disclosures in accordance with this DPA and/or as compelled by applicable law.

Annex B

Security Measures

SIA shall:

1. Provide a level of security (including appropriate Security Measures relating to the categories or nature of Customer Data) appropriate to protect against the harm that might result from a data breach, which shall include but not be limited to:
   a) ensure role-based access is granted only to those individuals needing access for the provision of the Licensed Software,
   b) ensure that suitable and effective authentication processes are established and used to protect Customer Data (e.g., multifactor authentication for privileged access or restricted information),
   c) back up Customer Data on a regular basis as required by the Customer and ensuring that any back up data is subject to appropriate Security Measures as necessary to protect the confidentiality, integrity and availability of Customer Data,
   d) encrypt, using industry standard encryption tools and key strengths, all records and files containing Customer Data that SIA:
      (i) transmits or sends (including wirelessly) across public networks,
      (ii) stores on laptops or storage media, or
      (iii) stores on portable devices.
   e) safeguarding the security and confidentiality of all encryption keys associated with encrypted Customer Data.

2. Establish, maintain and enforce a comprehensive information security program, that includes information security policies, hiring policies, privacy policies and data handling procedures consistent with industry standards and appropriate Security Measures or as mandated by Applicable Law, to protect the security, integrity and confidentiality of Customer Data against a data breach, which shall include but not be limited to:

   a) providing information security awareness and training programs covering its policies and practices to all employees' agents or other personnel that will have access to Personal Data,
   b) having a comprehensive, up to date and tested business continuity plan in place to protect the confidentiality, integrity and availability of Customer Data, and
   c) prohibiting employees, agents or other personnel from accessing or storing Customer Data remotely (e.g. from home or via their own electronic device or internet portal) other than through a secure electronic network and in accordance with an organisational remote working policy.

3. Not use Customer Data on systems that are in development or are in testing where the security controls are less protective than the controls identified in this Addendum.