

## **SignRequest Data Processing Addendum, Incorporating: GDPR and Standard Contractual Clauses**

This Data Processing Addendum ("DPA") forms part of the Sign Request Terms of Service ("Terms") and is applicable to customer's use of the SignRequest Service and reflects the parties' agreement with regard to the processing of Customer Personal Data. For good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

### **Article 1 – Definitions**

Definitions for capitalized terms used in this DPA shall apply to this DPA only and have the meaning ascribed to such terms in this section, regardless of whether the Terms are governed by different definitions for the same terms.

**“Adequacy”** means where the European Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question, ensures an adequate level of data protection.

**“Controller”** means the entity that determines the purposes and means of processing of Customer Personal Data.

**“Customer Personal Data”** means the Content (as defined in the Terms) which contains personal data.

**“Data Protection Legislation”** means the laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, as applicable to the processing of Customer Personal Data under this DPA.

**“Data Subject”** means the identified or identifiable person to whom Customer Personal Data relates.

**“EU GDPR”** means General Data Protection Regulation and is Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing of Directive 95/46/EC.

**“Processor”** means the entity which is processing Customer Personal Data on behalf of the Controller.

**“Subprocessor”** means any Processor engaged by SignRequest.

**“SignRequest”** means SignRequest B.V., a company registered with the Dutch Chamber of Commerce under number 61138008 and with offices at Singel 542, 1017AZ Amsterdam, Netherlands.

**“SignRequest Service”** means the Free Services or Paid Services (as defined by the Terms) provided by SignRequest.

**“UK GDPR”** means the UK Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020.

## Article 2 – Processing of Customer Personal Data

**A. Roles and Responsibilities.** The parties acknowledge that with regard to the processing of Customer Personal Data under the Data Protection Legislation and this DPA, customer is the Controller and SignRequest is the Processor. Each party will comply with the obligations applicable to it under the Data Protection Legislation with respect to the processing of Customer Personal Data.

**B. Customer’s Instruction and Authorization to Process Customer Personal Data.** SignRequest processes Customer Personal Data exclusively for and on behalf of the customer, in accordance with applicable Data Protection Legislation to provide the SignRequest Service as set forth in the Terms. Customer is solely responsible for the accuracy and legality of Customer Personal Data provided to SignRequest.

**C. Scope of Processing.** The types of Customer Personal Data and categories of Data Subjects that may be processed under this DPA are set forth in Annex 1 (“Stipulation of Personal Data and Data Subjects”).

**D. Data Protection Impact Assessment and Prior Consultation Assistance.** SignRequest will provide reasonable assistance to customer, as required by law and applicable to SignRequest’s role as a Processor, for customer to comply with customer’s obligations to perform a data protection impact assessment. In situations where customer’s processing of Customer Personal Data results in a high risk to the rights and freedoms of natural persons, SignRequest will provide reasonable assistance to customer as it seeks prior consultation from a supervisory authority.

## Article 3 – International Transfers of Personal Data

**A. GDPR.** SignRequest will process Customer Personal Data in accordance with EU and UK GDPR requirements applicable to SignRequest’s provision of the SignRequest Service.

**B. Transfer Mechanism for Data Transfers.** SignRequest makes available lawful data transfer mechanisms for cross-border transfers of Customer Personal Data or otherwise transfers Customer Personal Data to a country deemed Adequate by the European Commission. Subject to applicable Data Protection Legislation, SignRequest makes available the Standard Contractual Clauses set forth in Annex 2 to this DPA. Such data transfer mechanism shall apply to the SignRequest Service with respect to any transfer of Customer Personal Data under this DPA from the European Union, the European Economic Area (including its member states), Switzerland and the United Kingdom to countries which are not deemed to have Adequacy (to the extent that such transfers are subject to such Data Protection Legislation).

### C. Additional Terms Applicable to Standard Contractual Clauses

- (1) The Standard Contractual Clauses set forth in Annex 2 and the terms set forth in this Section C shall apply to the legal entity that has executed the Standard Contractual Clauses as a data exporter. For the purposes of Standard Contractual Clauses, customer shall be the data exporter and SignRequest shall be deemed the data importer. This DPA is the customer’s instructions to SignRequest for the processing of Customer Personal Data. Any additional or alternate instructions must be agreed upon separately in writing. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the customer to process Customer Personal Data: (a) processing in accordance with the Terms; (b) processing initiated by customers in their use of the SignRequest Service and (c) processing to comply with other reasonable documented instructions provided by customer (e.g., via email) where such instructions are consistent with the Terms and have been agreed to by SignRequest in writing.
- (2) The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with Article 7 (“Audits and Reports”) of this DPA.

- (3) Pursuant to Clause 5(h) of the Standard Contractual Clauses, customer acknowledges and expressly agrees that SignRequest and its affiliates may engage third-party Sub-processors in connection with the provision of the SignRequest Service in accordance with Article 9 of this DPA. Box shall make available to customer the current list of Sub-processors in accordance with 9(c) of this DPA. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that Box may engage new Sub-processors as described in Article 9(D) of this DPA.

## **Article 4 – Data Security**

**A. Security Controls.** SignRequest maintains appropriate technical and organizational measures to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access as described in Annex 3 (the “Description of the Technical and Organisational Measures”). As described in Annex 3, the security controls include measures to encrypt Customer Personal Data; to help ensure ongoing confidentiality, integrity, availability and resilience of SignRequest’s systems and services; to help restore timely access to Customer Personal Data following an incident; and for regular testing of effectiveness.

**B. Security Compliance of SignRequest Personnel.** SignRequest will take appropriate steps to ensure compliance with the security controls by its employees, contractors and Subprocessors to the extent applicable to their scope of performance, including ensuring that all persons authorised to process Customer Personal Data have agreed to an appropriate obligation of confidentiality.

## **Article 5 – Data Incidents**

After becoming aware of an accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to Customer Personal Data transmitted, stored or otherwise processed by SignRequest or its Subprocessors (“Data Incident”), SignRequest will notify Customer without undue delay (“Data Incident Notification”). SignRequest will take reasonable steps to: (i) provide Customer with a description of the Data Incident and the type of data that was the subject of the Data Incident; (ii) identify the cause of such Data Incident; and (iii) take the steps necessary and reasonable to remediate the cause of such Data Incident to the extent such remediation is within SignRequest’s reasonable control.

Data Incident Notification will be delivered to the administrator(s) of Customer’s SignRequest Service account (“Notification Email Address”). Customer is solely responsible for ensuring that the Notification Email Address associated with Customer’s account is current and valid.

## **Article 6 – Deletion and Return of Customer Data**

Upon cancellation or termination of the SignRequest Service, SignRequest provides customer with controls to enable customer to retrieve, rectify, or delete Customer Personal Data pursuant to the Terms. SignRequest will provide reasonable assistance to Customer where necessary to assist with such obligations.

## **Article 7 – Audits and Reports**

**A. Reports.** SignRequest uses independent external auditors to verify its security measures for security certifications. SignRequest has received ISO 27001 certification and will maintain this certification or its substantial equivalent for the term of this DPA. Upon customer’s written request and subject to confidentiality obligations set forth in the Terms, SignRequest agrees to make available this certification in order to demonstrate that SignRequest’s technical and organizational measures are sufficient and in order to ensure that SignRequest complies

with the technical and organizational measures as required in accordance with the applicable Data Protection Legislation.

**B. Audit.** Upon customer's request, and subject to the confidentiality obligations set forth in the Terms, SignRequest will make available to customer information regarding SignRequest's compliance with its obligations set forth in this DPA in the form of SignRequest's ISO 27001 certification.

## **Article 8 – Data Subject Rights**

**A. Data Subject Requests.** SignRequest will assist the Customer with requests from a Data Subject in relation to Customer Personal Data in accordance with Data Protection Legislation.

**B. Third-Party Requests.** In the event SignRequest receives a request from a third-party to provide access to Customer Personal Data, SignRequest will inform the Customer in writing before providing access to the third-party so the Customer can assess the legitimacy of the request, unless SignRequest is prohibited by law from doing so.

## **Article 9 – Subprocessors**

**A. Consent to Subprocessors.** Customer explicitly gives consent to the use of Subprocessors by SignRequest in order to allow SignRequest to fulfill its contractual obligations under this DPA and to provide certain services on SignRequest's behalf, such as support services.

**B. Subprocessor Commitments.** SignRequest undertakes to enter into a written agreement with any applicable Subprocessor in accordance with the requirements set out under applicable Data Protection Legislation. SignRequest will restrict the Subprocessor's access to only what is necessary to maintain the SignRequest Service or to provide the SignRequest Service to Customers. Customer hereby consents to SignRequest's use of Subprocessors as described in this Article 8 (Subprocessors). SignRequest will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Subprocessors.

**C. Current Subprocessors.** Information regarding SignRequest's current Subprocessors, including their location and services can be found in the SignRequest Privacy Notice found here: <https://signrequest.com/en/privacy-policy>. This Subprocessor list may be updated from time to time by SignRequest in accordance with this Article 8 (Subprocessors).

**D. Changes to Subprocessors.** Customers may visit <https://signrequest.com/en/privacy-policy> for a current list of SignRequest's Subprocessors.

## **Article 10 – Liability and Indemnification**

Each Party's 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 provisions of the Terms.

## **Annex 1 – Stipulation of Personal Data and Data Subjects**

### **Processing Scope**

As provided in the DPA, SignRequest will process Customer Personal Data as necessary to provide the SignRequest Service pursuant to the Terms, in accordance with this DPA, and as instructed by Customer in their use of the SignRequest Service.

### **Categories of Data Subjects**

Subject to the determination and control by the Customer in its sole discretion, Customer may submit Customer Personal Data to the SignRequest Service relating to the following categories of Data Subjects including but not limited to:

- Customers
- Customer's users authorized by Customer to use the SignRequest Service
- Employees, agents, advisors, consultants of Customer (who are natural persons)
- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Website Visitors

### **Types of Customer Personal Data**

Subject to the determination and control by the Customer in its sole discretion, Customer may submit Customer Personal Data to the SignRequest Service including but not limited to the following types of Customer Personal Data:

- Full name
- Contact information (address, phone, email)
- Social media accounts
- Photos
- Civil service numbers
- Resumes
- Personal life data (date of birth, marital status, gender, language)
- Financial data
- IP address
- Physical location
- Visitor behavior

## Annex 2 – Standard Contractual Clauses (processor)

For the purposes of Article 26(2) of the Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: **The customer is the data exporter.**

Address:

Tel.:

Fax:

E-mail:

Other information needed to identify the organisation:

(the data **exporter**)

And

Name of the data importing organisation: **SignRequest B.V.**

Address: Singel 542, 1017AZ Amsterdam, Netherlands

Fax: N/A

E-mail: support@signrequest.com

Other information needed to identify the organisation: general business phone: +31 (0) 20 894 36 57

(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

### *Clause 1*

#### *Definitions*

For the purposes of the Clauses:

- (a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) *'the data exporter'* means the controller who transfers the personal data;

- (c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) *'the applicable data protection law'* 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 applicable to a data controller in the Member State in which the data exporter is established;
- (f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

## **Clause 2**

### ***Details of the transfer***

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

## **Clause 3**

### ***Third-party beneficiary clause***

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

#### ***Clause 4***

##### ***Obligations of the data exporter***

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 Annex 1 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

#### ***Clause 5***

##### ***Obligations of the data importer***

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract 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 Clauses, it will promptly notify the change to the data exporter as soon as it is



aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
  - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
  - (ii) any accidental or unauthorised access, and
  - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

## ***Clause 6***

### ***Liability***

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or

ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

#### ***Clause 7***

##### ***Mediation and jurisdiction***

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
  - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
  - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

#### ***Clause 8***

##### ***Cooperation with supervisory authorities***

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

#### ***Clause 9***

##### ***Governing Law***

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

#### ***Clause 10***

##### ***Variation of the contract***

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

## ***Clause 11***

### ***Subprocessing***

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses<sup>1</sup>. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established. ,
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

## ***Clause 12***

### ***Obligation after the termination of personal data processing services***

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

---

<sup>1</sup> This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

## Annex 3 - Description of the Technical and Organizational Measures

SignRequest will implement the controls listed below or their equivalent during the terms of this DPA:

**1. Access Controls.** SignRequest implements suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment. This will be accomplished by:

- Access authorizations for employees and third parties
- Key cards and access badges
- Protection and restriction of entrances and exits

**2. Access Control to Data.** SignRequest commits that persons entitled to use the data processing system will only access Customer Personal Data within the scope and to the extent covered by the respective access permission (authorization). This will be accomplished by:

- Locking of workstations
- Requirements for user authorization
- Confidentiality obligations
- Restriction of access to customer Personal Data to authorized personnel

**3. User Control.** SignRequest will implement suitable measures to prevent its data processing systems from being used by unauthorized persons. This will be accomplished by:

- Access authorization requirements
- Logging of events and activities
- Use of encryption where deemed appropriate by Processor
- Securing the areas in which data is located
- Separating production and test environment
- Auto log-off of user IDs when not used for a substantial period of time

**4. Transmission Control.** SignRequest will secure the Customer Personal Data processed through the use of the SignRequest Service. This will be accomplished by:

- Authenticating authorized personnel
- Encryption of Customer Personal Data in the external transmission

**6. Organizational Control.** SignRequest will maintain its internal organizational controls in a manner that meets the requirements of Data Protection Legislation. This will be accomplished by:

- Internal data processing policies and procedures, guidelines, instructions, and/or process descriptions for programming, testing and release
- Implementing an emergency / backup contingency plan

**7. Instructional Control.** The Customer Personal Data transferred by Controller to Processor may only be processed in accordance with the instructions of the Controller. This will be accomplished by:

- Policies and procedures for the Processor's employees