DATA PROCESSING AGREEMENT INSIGN 365

Standard contractual clauses between controllers and processors under Article 28 GDPR

As of 12.09.2023
Version 2.0.2

Data Processing Agreement

Between

Licensee of the online service inSign 365 according to the main contract

(hereinafter referred as to **Controller**)

and

inSign GmbH
Am Bäckeranger 2
85417 Marzling
Germany

(hereinafter referred as to **Processor**)

(hereinafter jointly the **Parties**, individually each a **Party**)

Preambel

The following clauses are the standard contractual clauses (Data Processing Agreement pursuant to Ar-ticle 28(3) of the GDPR), which comply with the requirements of Article 28(3) of the GDPR and were adopted by the EU Commission on June 4, 2021.

inSign GmbH is a company with its registered office in Germany. inSign uses the standard clauses for controllers and processors in the EU / EEA for the purpose of regulating data processing. The original text of the standard contractual clauses including the specified options can be accessed here: https://commission.europa.eu/law/law-topic/data-protection_en.

The standard contractual clauses provide for options in certain clauses for which inSign, as the processor, has already made a selection. The selected options are already implemented in the contract text for bet-ter readability. Omitted options are listed in Annex VI for the purpose of transparency. In all other re-spects, the standard contractual clauses have been adopted in unchanged form and only supplemented by individual provisions. Such additions are included exclusively in Annex V.

Section 1

Clause 1 – Purpose and Scope

a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of 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.

b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725

c) These Clauses apply to the processing of personal data as specified in Annex II.

d) Annexes I to IV are an integral part of the Clauses..

e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2 - Invariability of the Clauses

g) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

h) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3 – Interpretation

a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4 - Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 Optional – Docking clause

Nonobligatory.

Section II – Obligations of the Parties

Clause 6 – Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7 – Obligations of the Parties

7.1 Instructions

a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2 Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3 Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4 Security of processing

a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5 Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

a) The Parties shall be able to demonstrate compliance with these Clauses.

b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7 Use of sub-processors

a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 20 working days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is

subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8 International transfers

a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8 – Assistance to the controller

a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

b) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

   1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

   2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

   3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

   4) the obligations in Article 32 Regulation (EU) 2016/679/.

d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9 – Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679/, shall be stated in the controller's notification, and must at least include:

   1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

2) the likely consequences of the personal data breach;

3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

c) in complying, pursuant to Article 34 Regulation (EU) 2016/679 /, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

b) the details of a contact point where more information concerning the personal data breach can be obtained;

c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679 /

Section III – Final Provisions

Clause 10 – Non-compliance with the Clauses and termination

a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

   1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

   2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

   3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

Annex I – List of parties

Controller:

Licensee of the online service inSign 365

Processor:

inSign GmbH
Am Bäckeranger 2
85417 Marzling
Germany

Annex II – Description of the processing

The nature and purpose of the processing of Personal Data, the categories of Personal Data and the categories of Data Subjects shall be based on the description of services specified in the main contract.

Categories of data subjects whose personal data is processed

The Processor shall process personal data of the Client and of the Client's interested parties and customers.

Categories of personal data processed

The Processor processes personal data of all categories.

Sensitive data processed (if applicable)

The processor processes sensitive personal data (Art. 9 GDPR).

Nature of the processing

The nature of the processing shall be based on the description of services specified in the main contract.

Purpose(s) for which the personal data is processed on behalf of the controller

Electronic contracting with electronic signature.

Duration of the processing

The duration of the processing shall be based on the duration of services specified in the main contract.

Locations of processing

☒ Germany/EU

☒ Switzerland

☐ Other:

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing:

See Annex IV

Annex III – Technical and organizational measures including to ensure the security of the data

Introduction

The EU General Data Protection Regulation (GDPR) contains specifications about how personal data should be handled from a technical and organisational point of view. The aim is to provide data security. Data security is thus an additional and complementary aspect of data protection. The technical-organisational measures of subcontractors used that are necessary for your application are not included in this document and will be made available separately. Sub-contractors are selected carefully in accordance with Art. 28 GDPR and are monitored continuously.

Data security is regulated by law in Art. 32 (1) GDPR. These regulations require that technical and organisational measures are taken that are necessary to guarantee protection of personal data.

For automated processing (above all by hardware and software), the law identifies various control areas, each of which has various subsections:

(1) Confidentiality

(2) Integrity

(3) Availability and resilience

(4) Procedures for regular review, assessment and evaluation of effectiveness

(5) Pseudonymisation and encryption

For non-automated processing of personal data, the above control areas are not directly applicable according to the letter of the law. It is advisable, however, to organise data security on the basis of these control areas in such cases too, in order to provide the best possible protection. We shall present these measures below in order to meet our information obligations under Art. 32 (3) section (c).

Organisational matters

The employees used for data processing are obliged to maintain data secrecy and confidentiality pursuant to Art. 28 (3) sentence 2, section (b), 29, 32 (4) GDPR. The system administrators used for data processing are obliged to maintain confidentiality pursuant to Section 203 of the German Penal Code (StGB).

Some of the safeguarding measures on the following checklist relating to this area are not identified separately, as they fall within the area of responsibility of the sub-contractors or are not published in detail for reasons of maintaining security through confidentiality.

Security measures

The following points describe the technical and organisational measures that are operated by inSign:

Control objective	Measures
CONFIDENTIALITY	
1. Physical access control Measures that are appropriate to deny unauthorised persons physical access to data pro-	Electronic access control to the company building and central data processing systems (technical rooms) Electronic logging of all locking operations (key number and time stamp) Central allocation and documentation of allocation of locking rights

cessing systems in which personal data is processed or used.	Obligation to report loss and blocking of access rights Access to technical rooms only for authorised personnel with express consent of the management Presence of unauthorised persons in security areas only under supervision Careful selection of cleaning personnel Active network components outside the technical rooms are located only in locked security cabinets
2. IT access control Measures that are appropriate to prevent unauthorised persons from using data processing systems.	Protection of all data processing systems by means of a combination of username and password Change of default passwords for all system and infrastructure components Minimum requirements for password complexity by means of password guidelines Use of multi-factor authentication (MFA) Passwords must be changed if there is any suspicion that the password may be compromised (e.g. by disclosure, hacker attacks, etc.). Incorrect entry of the password is logged electronically and leads to temporary deactivation of the user account if it is repeated Encrypted storage of passwords Data processing systems block user input if there has been no interaction for a specific period Network segmentation, use of a demilitarised zone (DMZ) Access restriction for certain IP address ranges External access only via secure connections (VPN or TLS encryption) Implementation of regular software updates Automated vulnerability scans Logging of instances of administrative system access Documentation of configuration changes Regular review of access authorisations Operation of a separate guest network (guest WLAN) Use of spam filters and anti-malware programs on the server and client sides (including automatic updates) Functional restriction on the use of client systems and screen workstations (restrictive allocation of rights). Automatic network monitoring with alarm. Deactivating/blocking of services and network ports that are not required.

3. Rights control Measures to ensure that those authorised to use a data processing system can access only the data that is covered by their access rights and that personal data cannot be read, copied, modified or removed without permission when it is being processed or used and once it has been stored.	Automatic check of access rights by means of password Use of menus exclusively in accordance with authorisation Task and role-based rights concept Separation of usage and administration access External administrative access only in exceptional cases and under supervision by authorised personnel Implementation of regular software updates Automated vulnerability scans Logging of instances of administrative system access Documentation of configuration changes Personal data that is processed on behalf of the customer is stored encrypted using state of the art encryption methods Access to backups only possible for administrators Backups are stored encrypted using state of the art encryption methods Erasure and destruction of data storage devices in accordance with BSI recommendations
4. Separation rule Measures that ensure that data collected for different purposes can be processed separately.	Personal data collected for different purposes is processed separately Separation of test from production environments Separation of management network from production network Data for which processing has been commissioned is processed separately on independent, separate systems for each client
INTEGRITY	
1. Transfer control Measures that ensure that personal data cannot be read, copied, modified or removed during electronic transmission, or transport or storage on data storage devices and that make it possible to check and establish the points at which transmission of personal data by means of data transmission equipment is intended.	Transmission of personal data using suitable encryption procedures in accordance with the current state of the art (crypto concept) Encryption of mobile end devices using suitable encryption procedures in accordance with the current state of the art Erasure and destruction of data storage devices in accordance with BSI recommendations
2. Input control Measures that ensure that it is possible to verify and establish retrospectively whether and by	Logging for retrospective checking of data processing (systems) of: - Successful and failed login and log out procedures

whom personal data has been entered, modified or removed on data processing systems.	- Firewall logging (TCP/IP) - Logging of administrative activities via ticket system - Complete audit-log (inSign 365) Retention periods for backups are defined
3. Availability and resilience (Art. 32 (1) section (b) and (c) GDPR) Measures that ensure that personal data is protected against accidental destruction or loss and, in the event of a physical or technical incident, can be restored quickly.	All data processing equipment on which personal data is stored is located in ISO/IEC 27001:2013-certified data centers exclusively in Germany. Personal data is replicated across three availability zones within a data center using automated recovery and failover mechanisms. Automated monitoring of the entire system for availability and proper operation Logging of abnormal events and reporting to staff responsible Backup of personal data at least once a day on an independent, stand-alone backup system according to a data backup concept Automatic function monitoring of data backup Regular sampling to ensure that data can be restored Anti-malware programs are in place and are always kept up-to-date
PROCESS FOR REGULAR TESTING, ASSESSING AND EVALUATING EFECTIVENESS (Art. 25 (1) GDPR; Art. 32 (1) section (d) GDPR)	
1. Data protection management A data protection management system is in place. The DPMS includes the most important provisions of data protection legislation and a comprehensive structure for indicating the data protection measures.	
2. Default settings in accordance with data protection (Art. 25 (2) GDPR) As a matter of principle, only data that is appropriate and required for business purposes is collected and processed. Processes for automated data collection and processing are designed in such a way that only the data required can be collected.	
3. Order control Measures that ensure that personal data for which processing has been commissioned can be processed only in accordance with the Client's instructions.	All inSign employees who have access to systems receive instruction about data protection, undertake to maintain data secrecy and have accepted corresponding secrecy and confidentiality agreements as part of their employment contract. Should inSign deploy sub-contractors for data processing, certain provisions are implemented. These include ensuring that the technical-organisational measures of the sub-contractor are in place in accordance with Art. 28 GDPR and Art. 32 (1) GDPR. Prerequisites for entering into a sub-contracting arrangement: - Agreement for commissioned data processing in accordance with Art. 28 (3) GDPR

	- Data processing takes place exclusively within the EU, preferably in Germany - Service providers have appointed a company data protection officer and ensure through data protection organisation that that person is involved appropriately and effectively in the relevant operational processes - If possible certification of service providers according to ISO/IEC 27001:2013 - Checks and audits of the measures agreed with the service provider - Access rights for inSign employees are assigned restrictively to technical environments of service providers. - There is a contract template for Commissioned Data Processing for the transmission of personal data to external service providers which includes the appropriate control regulations.

PSEUDONYMISATION AND ENCRYPTION (Art. 32 (1) section (a) GDPR)
Use of appropriate cryptographic methods for encryption of communication (encryption in transit) and data at rest (encryption at rest) using a crypto concept.

Annex IV – List of sub-processors

The Client agrees to the appointment of the following sub-contractors by the Processor.

Service-Provider	Purpose	Type of data processed
BSI Business Systems Integration Deutschland GmbH Rheinstraße 97 64295 Darmstadt Germany	Implementation partner for SaaS operation.	All information required for the service.
Plusserver GmbH Venloer Str. 47 50672 Köln Germany	Provision of cloud computer centre services (in particular, network, computing, storage, backup)	Host name and IP address of customer servers, encrypted customer data.
gridscale GmbH Oskar-Jäger-Straße 173 50825 Köln Germany	Managed Service/ PaaS & IaaS Cloud Hosting.	Host name and IP address of customer servers. No original use or processing of customer data is carried out by the sub-contractor.
IONOS SE Elgendorfer Str. 57 56410 Montabaur Germany	Provision of cloud computer centre services (in particular, network, computing, storage, backup)	Host name and IP address of customer servers. No original use or processing of customer data is carried out by the sub-contractor.
rapidmail GmbH Augustinerplatz 2 79098 Freiburg i.Br. Germany	Provision of e-mail services	All information needed for e-mail communication.
CM.com Germany GmbH Dr. Eugen Schön Straße 35 97332 Volkach Germany	Provision of text messaging services	All information required for SMS communication.
die Bayerische IT GmbH Thomas-Dehler-Str. 25 81737 München Germany	Provision of cloud computer centre services for long-term archiving of documents	All the information needed for encypted processing of documents No original use or processing of customer data is carried out by the sub-contractor.
D-Trust GmbH Kommandantenstraße 18 10969 Berlin Germany	Provision of services for qualified electronic signatures (only if ordered as an option by the customer)	All the information needed to create, and sign with, qualified certificates

Swisscom Trust Services GmbH Konradstraße 12 8005 Zürich Switzerland	Provision of services for qualified electronic signatures (only if ordered as an option by the customer)	All the information needed to create, and sign with, qualified certificates
A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH Landstraßer Hauptstraße 1b, E02 1030 Wien Austria	Provision of services for qualified electronic signatures (only if ordered as an option by the customer)	All the information needed to create, and sign with, qualified certificates

Annex V – Additional Provisions

Costs for audits and support services

The Processor shall, at its own expense, conduct regular inspections and audits in accordance with its audit program under recognized standards and shall provide the Controller with the audit report of the audit upon request, at the time of the conclusion of the Agreement: ISAE 3402 Type II.

In addition to the right to audit pursuant to clause 7.6 lit. c), the Controller may carry out the audit of the processing activities covered by these clauses on an ad hoc basis. An occasion is, for example, a significant security incident on the part of the processor. The respective suspicious facts shall be presented by the Controller with the announcement of the review/inspection. The Processor may not claim any expenses or other remuneration for such event-related checks, inspections or support ser-vices if the Processor is solely responsible for the event.

In the event of other or unrelated checks, inspections or support services, the Processor may claim reasonable compensation from the Controller, provided that the Processor's human resources are tied up for this purpose.

Instructions, notifications or communication

If the parties are obliged under these clauses to send each other information, notifications or messages in writing, this must be done at least in text form (e.g. e-mail). The contact data of the controller or the processor specified in Annex I or other communication channels agreed between the parties shall be used for this purpose.

Authorized representative of the controller to issue instructions within the meaning of Article 28(3)a of the GDPR

Licensee of the online service inSign 365

Changes to the person(s) authorized to issue instructions must be made in writing or in text form. If the text form is used, the respective contractual partner must append its electronic signature in accordance with Art. 26 of the eIDAS Regulation.

Data protection officer of the controller for notifications within the meaning of Article 28(3) GDPR

Notifications within the meaning of Article 28(3) of the GDPR shall be sent to the Authorized representative.

Data protection officer of the Processor

Mr. Sascha Weller (lawyer)
Institute for Data Protection Law
Ziegelbräustraße 7
85049 Ingolstadt
Germany
datenschutz@bsi-software.com

Annex VI – Discarded Options

Clause 1 a

[OPTION 2: Article 29(3) and (4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data]

Clause 7.7 a

OPTION 1: PRIOR SPECIFIC AUTHORISATION: The processor shall not subcontract any of its pro-cessing operations performed on behalf of the controller in accordance with these Clauses to a sub-processor, without the controller's prior specific written authorisation. The processor shall submit the request for specific authorisation at least [SPECIFY TIME PERIOD] prior to the engagement of the sub-processor in question, together with the information necessary to enable the controller to decide on the authorisation. The list of sub-processors authorised by the controller can be found in Annex IV. The Parties shall keep Annex IV up to date.

Clause 8 c 4

[OPTION 2] Articles 33, 36 to 38 Regulation (EU) 2018/1725

Clause 9.1 b

[OPTION 2] Article 34(3) Regulation (EU) 2018/1725

Clause 9.1 c

[OPTION 2] Article 35 Regulation (EU) 2018/1725

Clause 9.2

[OPTION 2] Articles 34 and 35 of Regulation (EU) 2018/1725