

Declaration with respect to job data processing in compliance with international data privacy guidelines and the German Data Protection Law (BDSG)

Dated: October 26th 2010

AuthentiDate Deutschland GmbH (hereafter referred to as the "Service Provider") hereby issues the following Declaration dealing with the processing of data from clients as part of the SIGNAMUS web services of AuthentiDate Deutschland GmbH (job data processing). This Declaration is an integral part of a client's job data processing order to AuthentiDate Deutschland GmbH as part of the SIGNAMUS web services and contains the rights and obligations of clients and service providers.

1 Definitions

The Service Provider within the meaning of the Declaration is AuthentiDate Deutschland GmbH.

The Clients within the meaning of this Declaration are commercial companies, public and non-public organisations and institutions that have concluded a written agreement with the Service Provider for the provision of services from SIGNAMUS web services.

Order data processing is a service that consists in the processing of data or documents by SIGNAMUS web services agreed as part of a written contractual relationship.

2 Binding international rules and national data protection laws

SIGNAMUS web services processes data from practically all the countries in the world; i.e. worldwide. All data protection measures are planned and implemented with an international focus too.

Unfortunately, binding international rules on data protection (international privacy) do not currently exist. So far only non-binding international recommendations, declarations of intent and initiatives exist. A current summary of international recommendations and national rules on the subject of data protection may be found online under www.privacyinternational.org.

In order to provide all SIGNAMUS customers with the highest level of data protection at all times in spite of the absence of binding international rules, AuthentiDate has complied with the legal data protection provisions of the country (Germany) that has the leading and strictest data protection provisions in the whole world. Compliance with these strictest provisions in the world guarantees the security of data throughout the world.

Additional information on the German Data Protection Law as well as the text of the law may be found in German and in English language online on the web site of the German Federal Officer for Data Protection and Freedom of Information under www.bfdi.bund.de.

In what follows the Declaration therefore deals with the particular requirements of these special legal requirements.

3 General

(1) The Service Provider processes personal data on behalf of the Client. The Client is required to select the Service Provider as part of his duties of care set out in § 11 of the German Data Protection Law (BDSG). Permission for job data processing is conditional on the Client awarding the Service Provider a written order. In accordance with the parties' intentions and particularly those of the Client, this contract contains the written order to perform this service within the meaning of § 11 of the German BDSG and establishes the parties' rights and obligations with regard to data processing.

(2) Wherever the term "data processing" or "processing" (of data) is used, this shall mean the processing of personal data in general.

4 Subject matter of the services

The Client's order to the Service Provider includes the following work and/or services:

The generation of electronic signatures, checking electronic signatures, storing, archiving and converting for data sets, documents or other data that might contain personal data.

5 The Client's rights and obligations

(1) The Client is the responsible unit (§ 3 section 7 of the German BDSG) for the job processing of data by the Service Provider. The Client alone is responsible for assessing the legality of the data processing.

(2) As the responsible unit, the Client is responsible for safeguarding the rights of those affected. The rights of those affected must be enforced vis-à-vis the Client. The Client awards all orders or part orders in writing. Changes to the processing subject matter and to procedures will be agreed jointly.

(3) The Client has the right before data processing begins and thereafter regularly to assure himself of compliance with the technical and organisational measures taken by the Service Provider to ensure data security. The Client is required to document the results in some suitable manner.

(4) The Client has the right to issue instructions with regard to the nature, scope and processes of data processing. The Client must immediately confirm instructions given verbally or in text form (e.g. e-mail) in writing.

(5) The Client may appoint persons entitled to issue instructions. The Client will provide the exact names of persons entitled to issue instructions should the Service Provider process sensitive data for the Client.

The Client will inform the Service Provider in writing should the persons he appoints entitled to issue instructions change.

(6) The Client will inform the Service Provider immediately should he establish errors or irregularities in connection with the processing of personal data by the Service Provider.

6 The Service Provider's obligations

(1) The Service Provider will process personal data solely as part of agreements made. The purpose, nature and scope of the data processing will be governed solely by the Client's instructions. Unless the Client has given his consent in writing, the Service Provider is forbidden from processing data contrary to the principle.

(2) The Service Provider will support the Client in carrying out checks and cooperate in conducting these checks fully and quickly.

(3) Documents and data sets with personal data that are no longer required will be automatically returned to the employer without their having to be requested, or destroyed in a manner stipulated by the data protection legislation.

(4) Should the Service Provider be required to appoint a company data protection officer within the meaning of § 4f of the German BDSG, he confirms this appointment with this Declaration and will provide the Client with the name of this person in writing or in text form (e.g. e-mail) if required to do so.

(5) The Service Provider warrants that in job processing personal data, all agreed measures will be carried out according to contract. He also warrants that the data processed will be kept separate from other data (see section 8 of the attachment to § 9 of the German BDSG).

(6) The Service provider is required to organise his company and business processes in such a way that the data processed on behalf of the Client are stored in the required manner and protected from becoming known by unauthorised third parties.

(7) The Service Provider will inform the Client immediately should an instruction issued by the Client in his opinion contravene provisions of the law. The Service Provider is entitled to suspend carrying out the instruction(s) concerned until the Client confirms or amends them.

(8) The Service Provider is required to notify the Client immediately of every infringement of the regulations relating to data protection or the agreed contractual agreements and/or the Client's instructions that has occurred during the processing of the data by the Service Provider or other persons involved in their processing.

(9) The Service Provider is required to inform the Client as appropriate should data be processed on behalf of the Client outside the Service Provider's business premises or on sub-contractors' premises. The Service Provider is required to ensure compliance with the relevant provisions of the BDSG in this situation too.

(10) The Service Provider will appropriately label data he processes on behalf of the Client. The Service Provider will label the data with the relevant purpose should it be processed for different purposes.

(11) The Service Provider will cooperate in the Client's preparation of lists of processes. He will provide the Client with the required information in a suitable manner.

(12) The Service Provider may give the Client the name(s) of person(s) entitled to receive the Client's instructions.

(13) This will not affect any provisions agreed with respect to payment for additional expenses incurred by the Service Provider in carrying out the Client's instructions.

7 Scope of the authority to issue instructions

(1) The Client is entitled at any time to issue complementary instructions to the Service Provider with respect to the purpose, nature and scope of the processing of data. The instructions must be issued in writing. The Service Provider must be allowed an adequate period of time in which to implement instructions.

(2) This will not affect any provisions agreed with respect to payment for additional expenses incurred by the Service Provider in carrying out complementary instructions carried out by the Client.

8 Right to audit

(1) The Client is entitled to appoint independent third parties, such as for example auditors or companies specialised in data protection audits, to audit Service Provider's compliance with legal data protection requirements and/or with the contractual provisions agreed between the parties and/or with the Client's instructions. The Client will pay the costs of appointing third parties for auditing.

(2) The Client is required to ensure that the independent third party treats all information and results he receives as part of these checks confidentially. Companies, which are wholly or partly in competition with the Client may not be appointed to audit ordered by the Client as described in section 1.

(3) The Service Provider is required to provide independent third parties appointed by the Client with the information necessary for auditing described in section 1.

(4) Third parties appointed by the Client may demand an inspection of the data processed by the Service Provider on behalf of the Client as well as of documentation on the data processing systems used.

(5) The independent third party appointed by the Client may perform the audit described in section 1 on the Service Provider's premises during normal business hours having previously given adequate notice. Adverse effects to regular business processes shall be avoided.

9 Data Secrecy

(1) The Service Provider is required to safeguard data secrecy as required by § 5 of the German BDSG in processing data on behalf of the Client. The Service Provider undertakes to comply with the same rules regarding data secrecy as bind the Client.

(2) The Service Provider gives an assurance that he is acquainted with the relevant regulations on data secrecy and with their application. The Service Provider also gives an assurance that he will acquaint his employees involved in the work with the data protection rules applicable to them and that he will bind them to data secrecy within the meaning of § 5 of the German BDSG.

10 Safeguarding the rights of those affected

(1) The Client alone is responsible for safeguarding the rights of those affected.

(2) Should the Service Provider's cooperation be necessary in order for the Client to safeguard the rights of those concerned – especially with respect to information, reporting, blocking or deleting data - the Service Provider will take the necessary measures in accordance with the Client's instructions.

(3) This will not affect any provisions agreed with respect to payment for additional expenses incurred by the Service Provider in carrying out complementary instructions carried out by the Client.

11 Obligations maintaining non disclosure

(1) Both parties undertake to keep secret all information they receive in connection with the fulfilment of this job indefinitely and only to use this information in order to fulfil the contract. Neither of the parties is entitled to use this information wholly or partially for any purposes than those just named or to disclose this information to third parties.

(2) The above obligation will not apply to information that one of the parties can prove to have obtained from third parties not obliged to maintain secrecy or information that is publicly known.

12 Technical and organisational data security measures

(1) The Service Provider undertakes to the Client that he will take the following technical and organisational measures required to comply with the applicable data protection regulations (see also the requirements set out in §9 of the German BDSG):

a) Entry control

Measures with which unauthorised persons are prevented from obtaining access to data processing equipment with which personal data is processed or used:

Access to the SIGNAMUS systems is protected by a multi-layer zone model. These zones must be passed from the exterior to the interior in order to acquire access to the SIGNAMUS systems.

Every zone is protected by electronic or physical access control mechanisms that only allow those entitled to access to pass. The entitlements become ever more restrictive as one passes from the outside to the interior.

The principle of minimum privileges is basically applied, so that people only acquire access entitlement to those zones that are absolutely necessary in order to allow them to do their work.

The records of those obtaining electronic access are stored and may, subject to the involvement of the company data protection officer, be assessed.

b) Control of access to the system

Measures by which the use of the data processing equipment by unauthorised persons is prevented:

Access to the SIGNAMUS systems is protected at several levels. Access is only possible after successful authentication for the operating system. Each user has his own user account to which only he knows the password. A complexity guideline that ensures the quality of the passwords used is applied for passwords.

A record is kept of successful and failed attempts to obtain access to the systems.

The SIGNAMUS systems are protected from unauthorised network links by reliable firewall architecture. Only authorised administrators can acquire administrative remote access by means of a coded connection with dual-factor authorisation.

c) Control of access to protected data

Measures that ensure that those authorised to use a data processing system may only obtain access to data to which their entitlement legitimises them and that personal data may not be read, copied, changed or erased during processing, use and after storing:

Since SIGNAMUS carries out automatic job data processing, it is normally not necessary that the staff of AuthentiDate International AG have access to personal data in order to process, use and store this data.

Access to this data occurs only should it be necessary to search for an error.

Appropriate file system entitlements are used to restrict access to the data to what is absolutely necessary for processing purposes.

d) Control of the transfer of data

Measures that ensure that personal data is not read, copied, changed or deleted in an unauthorised manner during electronic transmission or whilst being transported or stored on data media and that can check and establish at which points a transfer of personal data by data processing installations is foreseen:

All data that is transferred by external means of transmission, e.g. by Internet, are coded during transfer to and from the SIGNAMUS systems. An electronic record is kept of all data transfers.

The unauthorised reading, copying or amendment of the data is prevented by access controls and their protective mechanisms.

e) Input control

Measures that ensure that it can be checked subsequently whether and by whom personal data has been entered into the data processing system, altered or removed:

The system technically excludes the anonymous manual input or collection of data for further processing in the SIGNAMUS system. The transfer of data to the SIGNAMUS system for further processing purposes require successful prior authentication. An electronic record is kept of all data transfers.

Non-authorised transfers are rejected before the data can be transferred. The system technically excludes changes to or the deletion of data by external systems.

f) Control of the order processed

Measures that ensure that personal data put out to job processing can only be processed in accordance with the client's instructions:

All data transferred to SIGNAMUS System are labelled by order. This ensures that they can only be processed according to the client's instructions and in accordance with the agreed purpose of the contract. Electronic records are made of the processing.

g) Control of accessibility

Measures that ensure that personal data is protected from accidental destruction or loss:

All data sent to the SIGNAMUS system for further processing are backed up during processing and/or archiving (should this have been agreed). All data is periodically stored on data media and a copy kept outside the company. This prevents the loss or destruction of data.

h) Control of separation

Measures that ensure that data gathered for different purposes can be processed separately.

The Client will transmit all data through separate input lists that only the relevant client has by way of the access data. Different clients' data will be logically stored and processed separately from each other. A client is unable to acquire access to or to inspect other clients' data.

13 End of the assignment

The Service Provider is required to return to the Client all documents and data acquired and the results of processing and use generated related to job processing after the job has ended. The Service Provider's data media must be physically erased afterwards. This also applies to any data back-ups in the Service Provider's possession. The deletion must be suitably documented. Test and waste material must be immediately destroyed or physically erased.

14 Concluding provisions

(1) The Service Provider is required to inform the Client immediately should the Client's property be endangered whilst in the Service Provider's possession premises by measures taken by third parties (for instance, through attachment or confiscation) as a result of insolvency proceedings or other events. The Service Provider will immediately inform creditors that data is involved that is being job processed.

(2) Side-agreements must be in writing.

(3) The plea of the right to withhold processed data and the associated data media within the meaning of § 273 of the German Civil Code is excluded.

Düsseldorf, October 26th 2010



Jan C. Wendenburg
CEO

AuthentiDate Deutschland GmbH (Service Provider)
Rethelstrasse 47
40237 Düsseldorf