Terms and Conditions for Allegion Data Processing and Transfer

These Terms and Conditions for Allegion Data Processing and Transfer ("**Addendum**") is entered into by and between **YOU** **("Supplier"):** and (ii) Schlage Lock Company LLC on behalf of itself and its data controller affiliates (collectively, "**Customer**"). This is an Addendum to the agreement ("**Agreement**" or **Underlying Agreement**") entered into by and between Customer or its affiliate and Supplier or Supplier's affiliate. In the event of a conflict between this Addendum and the Agreement, this Addendum shall control.

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Authorised Subprocessors**" means (a) those Subprocessors set out in the Agreement, if any **(Authorised Subprocessors)**; and (b) any additional Subprocessors consented to in writing by the Customer in accordance with section 5.1;

1.1.2 "**Process/Processing**", "**Data Controller**", "**Data Processor**", "**Data Subject**", **"Personal Data", "Personal Data Breach"** and "**Special Categories of Personal Data**" shall have the same meaning as in the Data Protection Laws;

1.1.3 "**Data Protection Laws**" means any laws, rules or regulations in relation to any Personal Data which is Processed in the performance of the Underlying Agreement, including, without limitation, the EU Data Protection Directive 95/46/EC until 25 May 2018 and the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") on and from 25 May 2018), in each case together with all laws implementing or supplementing the same and any other applicable data protection or privacy laws;

1.1.4 "**EEA**" means the European Economic Area;

1.1.5 "**Customer Personal Data**" means the data described in Annex 1 and any other Personal Data Processed by Supplier or any Supplier affiliate on behalf of the Customer or any Customer affiliate pursuant to or in connection with the Agreement;

1.1.6 "**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of personal data to Processors established in third countries, as approved by the European Commission in Decision 2010/87/EU, or any set of clauses approved by the European Commission which amends, replaces or supersedes these ;

1.1.7 "**Subprocessor**" means any Data Processor (including any third party and any Supplier Affiliate) appointed by Supplier to Process Customer Personal Data on behalf of the Customer or any Customer affiliate;

1.1.8 "**Supervisory Authority**" means (a) an independent public authority which is established by a Member State pursuant to Article 51 GDPR; and (b) any similar regulatory authority responsible for the enforcement of Data Protection Laws;

2. Processing of the Customer Personal Data

2.1 Supplier shall only Process the types of Customer Personal Data relating to the categories of Data Subjects for the purposes of the Agreement and for the specific purposes in each case as set out in **Annex 1 (Details of Processing of Customer Data)** to this Addendum and shall not Process, transfer, modify, amend or alter the Customer Personal Data or disclose or permit the disclosure of the Customer Personal Data to any third party other than in accordance with the Customer's documented instructions (whether in the Agreement or otherwise) unless Processing is required by EU or Member State law to which Supplier is subject, in which case Supplier shall to the extent permitted by such law inform the Customer of that legal requirement before Processing that Personal Data. Supplier shall assist Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR

taking into account the nature of Processing and the information available to Supplier. Supplier shall comply with all Data Protection Laws.

3. Supplier Personnel

3.1 Supplier shall take all necessary steps to ensure the reliability of any employee, agent or contractor who may have access to the Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to access the relevant Customer Personal Data, as strictly necessary for the purposes set out in section 2.1 above in the context of that individual's duties to Supplier, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Supplier shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

4.2 Without limitation to section 4.1, Supplier shall implement and maintain each of the technical and organisational measures listed in **Annex 2 (Technical and Organisational Measures)**.

5. **Subprocessing**

5.1 Subject to section 5.2, Supplier shall not engage any Data Processors to Process Customer Personal Data other than with the prior written consent of the Customer, which the Customer may refuse in its absolute discretion. Supplier shall include terms in the contract between Supplier and each Subprocessor which are materially the same as those set out in this Addendum. Upon request, Supplier shall provide a copy of its agreements with Subprocessors to the Customer for its review.

5.2 As at the Addendum Effective Date, the Customer hereby authorises Supplier to engage those Subprocessors set out in the Agreement, if any.

6. Data Subject Rights

6.1 Supplier shall promptly notify the Customer if it receives a request from a Data Subject or a Supervisory Authority under any Data Protection Laws in respect of Customer Personal Data.

6.2 Supplier shall co-operate as requested by the Customer to enable the Customer to comply with any exercise of rights by a Data Subject under any Data Protection Laws in respect of Customer Personal Data and comply with any assessment, enquiry, notice or investigation under any Data Protection Laws in respect of Customer Personal Data or this Addendum, where applicable, providing such assistance as is reasonably requested by the Customer to enable the Customer to comply with the relevant request within the timescales prescribed by the Data Protection Laws.

7. **Personal Data Breach**

7.1 Supplier shall notify the Customer promptly, and in any case within twenty-four (24) hours, upon becoming aware of or reasonably suspecting a Personal Data Breach providing the Customer with sufficient information which allows the Customer to meet any obligations to report a Personal Data Breach under the Data Protection Laws.

7.2 Supplier shall co-operate with the Customer and take such reasonable commercial steps as are directed by the Customer to assist in the investigation, mitigation and remediation of each Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

8.1 Supplier shall provide reasonable assistance to the Customer with any data protection impact assessments which are required under Article 35 GDPR and with any prior consultations to any supervisory authority of the Customer or any Customer affiliate which are required under Article 36 GDPR, in each case solely in relation to Processing of Customer Personal Data by Supplier on behalf of the Customer and taking into account the nature of the Processing and information available to Supplier.

9. Deletion or Return of Customer Personal Data

9.1 Supplier shall promptly and in any event within 90 (ninety) calendar days of the earlier of: (i) cessation of Processing of Customer Personal Data by Supplier; or (ii) termination of the Agreement, at the choice of the Customer (such choice to be notified to Supplier in writing) either:

9.1.1 return a complete copy of all Customer Personal Data to the Customer by secure file transfer in such format as notified by the Customer to the Supplier and securely wipe all other copies of Customer Personal Data Processed by Supplier or any Authorised Subprocessor; or

9.1.2 Securely wipe all copies of Customer Personal Data Processed by Supplier or any Authorised Subprocessor,

and in each case provide written certification to the Customer that it has complied fully with this section 9.

10. Audit rights

10.1 Supplier shall make available to Customer all information necessary to demonstrate Supplier's compliance with the obligations of Supplier set forth in this Addendum and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by the Customer. Supplier shall immediately inform the Customer if, in its opinion, an instruction pursuant to this section 10 (Audit Rights) infringes the GDPR or other EU or Member State data protection provisions.

11. International Transfers of Customer Personal Data

11.1 Supplier shall not Process the Customer Personal Data nor permit any Authorised Subprocessor to Process the Customer Personal Data in a country located outside of the European Union (a "**Restricted Country**"), unless authorised in writing by the Customer in advance. In addition, Supplier shall not Process the Customer Personal Data nor permit any Authorised Subprocessor to Process the Customer Personal Data in a country located outside of the home country of the Customer group entity providing Customer Personal Data, unless authorised in writing by the Customer in advance (and, for clarity, if the Customer group entity home country is outside of the European Union, advance written consent from Customer is also required for Processing outside of the European Union). If Supplier Processes Customer Personal Data or permits any Authorised Subprocessor to Process the Customer Personal Data in a country located outside of the European Union, the parties agree to enter into **Annex 3 (Standard Contractual Clauses)**. If Supplier Processes Customer Personal Data in Switzerland or pertaining to Swiss citizens or residents, the parties agree to enter into **Annex 4 (Swiss Model Clauses).** If Supplier Processes Customer Personal Data in Germany or pertaining to German citizens or residents, the parties agree to enter into **Annex 5 (German Companion Agreement)**. If Supplier Processes Customer Personal Data in Poland or pertaining to Polish citizens or residents, the parties that **Annex 6 (Poland Security)** applies. If Supplier Processes Customer Personal Data in Italy or pertaining to Italian citizens or residents, the parties agree that **Annex 7 (Italy Security)** applies.

11.2 When requested by the Customer, Supplier shall promptly enter into (or procure that any relevant Subprocessor of Supplier enters into) an agreement with the Customer or a Customer affiliate as Data Protection Laws might require, in respect of any Processing of Customer Personal Data in a Restricted Country, which terms shall take precedence over those in this Addendum.

12. General Terms

12.1 The parties agree that this Addendum shall terminate automatically upon termination of the Agreement or expiry or termination of all service contracts entered into by Supplier with the Customer pursuant to the Agreement, whichever is later. Any obligation imposed on Supplier under this Addendum in relation to the Processing of Personal Data shall survive any termination or expiration of this Addendum.

12.2 Conflicts with any other provision of the Agreement notwithstanding, a violation of this Addendum by Supplier and Supplier's indemnification, defense and hold harmless obligations below are not subject to any limitation on the type or amount of Supplier's liability or any other limitation on Supplier's liability. Supplier shall indemnify, defend and hold Customer and its affiliates and its and their respective directors, officers, representatives, agents, successors and assigns harmless from and against any and all settlements, judgments, awards, fines, penalties, sanctions, interest, liabilities, losses, costs, damages and expenses, including, without limitation, reasonable attorneys' fees and disbursements and court costs, arising from or related to Supplier's violation of this Addendum. Supplier shall maintain sufficient insurance coverages to satisfy its obligations under this Addendum.

ANNEX 1: DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

This Annex 1 includes certain details of the Processing of Customer Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Customer Personal Data

As instructed by Allegion in writing in the Agreement or otherwise

The nature and purpose of the Processing of Customer Personal Data

As instructed by Allegion in writing in the Agreement or otherwise

The types of Customer Personal Data to be Processed

As instructed by Allegion in writing in the Agreement or otherwise

The categories of Data Subject to whom the Customer Personal Data relates

As instructed by Allegion in writing in the Agreement or otherwise – will be customer data, former customer data, end user data, former end user data, employee data, former employee data, applicant data, supplier data and/or contractor data or any other data as instructed by Allegion

Special categories of data (if appropriate)

As instructed by Allegion in writing in the Agreement or otherwise

Processing operations (as applicable)

As instructed by Allegion in writing in the Agreement or otherwise

ANNEX 2: TECHNICAL AND ORGANISATIONAL MEASURES

In addition to any measures agreed to by the Supplier, the Supplier undertakes to institute and maintain the following data protection measures:

1. Access control of persons

The Processor shall implement suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment until the Personal Data transferred by the Controller are processed.

This shall be accomplished by:

Establishing access authorizations for employees and third parties, including the respective documentations;

Code card passes;

Restrictions on keys;

Regulations for third parties;

Regulations on key codes;

Identification of the persons having access authority;

Security alarm system or other appropriate security measures even after the working time;

Securing the decentralized data processing equipment and personal computers;

Protection and restriction of access path.

2. Access control to Personal Data

The Processor commits that the persons entitled to use the data processing system are only able to access the Personal Data within the scope and to the extent covered by the respective access permission (authorization).

This shall be accomplished by:

Locking of terminals;

Allocation of individual terminals and/or terminal user and identification characteristics exclusive to specific functions;

Functional and/or time restricted use of terminals and/or terminal users and identification characteristics;

Regulations for user authorization;

Obligation to comply with data secrecy;

User codes for Personal Data and programs;

Coding routines for files;

Differentiated access regulations (e. g. partial blocking);

Regulations for the organisation of files;

Logging and analysis of use of the files;

Special control regarding the application of help programs as far as they are able to evade security measures;

Controlled destruction of data media;

Work instructions for templates for the registration of Personal Data;

Checking, adjustment and controlling systems;

Processes for the checking and release of programs.

3. User Control

The Processor shall implement suitable measures to prevent its data processing systems from being used by unauthorized persons by means of data transmission equipment. In addition, the Processor shall implement suitable measures to prevent unauthorized reading, copying, alteration or removal of the data media, unauthorized input into memory, reading, alteration or deletion of the stored Personal Data.

This shall be accomplished by:

Authorization concept;

Terminal with access user key;

Identification of the terminal and / or the terminal user to the system of the Processor;

Automatic turn-off of the user ID when several erroneous passwords where entered;

Log file of events (monitoring of break-in attempts);

Issuing and safeguarding the identification codes;

Dedication of individual terminals and/or terminal users;

Identification characteristics exclusive to specific functions;

Authentication of the authorized personnel;

Protective measures for the data input into memory as well as for the reading, blocking and deletion of stored Personal Data;

Use of encryption for critical security files;

Specific access rules for procedures, control cards, process control methods, program cataloguing authorization;

Guidelines for data file organisation;

Keeping records of data file use;

Separation of production and test environment for libraries and data files;

Providing that entries to data processing facilities (rooms, housing, computer hardware and related equipment) are capable of being locked;

Automatic log-off of user IDs that have not been used for a substantial period of time;

Designating the areas in which data media may / must be located;

Designating the persons in such areas for authorized remove of data media;

Controlling the removal of data media;

Securing the areas in which data media are located;

Release of data media only to authorized persons;

Control of files, controlled and documented destruction of data media;

Policies controlling the production of backup copies.

4. Transmission control

The Processor shall be obliged to enable the verification and tracing of the locations/destinations to which the data subject's Personal Data are transferred by the utilization of the Processor's data communication equipment/devices.

This shall be accomplished by:

Authentication of the authorized personal;

In-house verification requirements (four-eye principle);

Designating the areas in which data media may / must be located;

Controlling the removal of data media;

Designating the persons in such areas who are authorized to remove data media;

Control of files;

Locking of confidential data media;

Security lockers;

Prohibition of taking bags etc. within the secure area;

Control of destruction of data media;

Policies controlling the production of backup copies;

Documentation of the transfer programs;

Documentation of the retrieval and transmission programs;

Documentation of the remote locations/destinations to which a transmission is intended and the transmissions path (logical path);

Authorization policy;

Encryption of the Data for online transmission or transport by means of data carries (tapes and cartouches);

Monitoring of the completeness and correctness of the transfer of Data (end to end check);

Encryption;

Courier services, personal pickup, accomplishing of the transport;

Control of plausibility;

Control of completeness and correctness;

Deletion of remaining Personal Data before change of data media.

5. Input Control

The Processor shall provide for the retroactive ability to review and determine the time and the point of the data subject's Personal Data entry into the Processor's data processing system.

This shall be accomplished by:

Proof of Processor's organisation of the input authorization;

Electronic recording of entries;

Electronic recording of data processing, in particular usage of Data.

6. Organisation control

The Processor shall maintain its internal organisation in a manner that meets the requirements of this Agreement.

This shall be accomplished by:

Internal data processing policies and procedures, guidelines, work instructions, process descriptions and regulations for programming, testing and release, insofar as they relate to the Personal Data transferred by the Controller;

Formulation of a data security concept;

Industry standard system and program examination;

Formulation of an emergency plan (backup contingency plan).

7. Instructional control

The Data transferred by the Controller to the Processor may only be processed in accordance with the instructions of the Controller.

This shall be accomplished by:

Binding policies and procedures for the Processor's employees;

Upon request, access will be granted to those of the Controller's employees and agents who are responsible for monitoring the Processor's compliance with this Agreement.

8. Control of separation of Personal Data

The Processor shall implement suitable measures to allow the separate processing of Personal Data which have been collected for different purposes.

This shall be accomplished by:

Storage of the Personal Data in separated data collectors (physical separation);

Authorization policy (logical separation);

Separation of the Personal Data, which have been stored under an alias (pseudonym) from the original Personal Data.

ANNEX 3: STANDARD CONTRACTURAL CLAUSES

For the purposes of Article 26(2) of 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

Schlage Lock Company LLC on behalf of and for the benefit of all data exporter affiliate(s) of the Schlage Lock Company LLC, who are each entitled to enforce the Clauses as independent data exporters.

Address: 11819 N. Pennsylvania Street, Carmel, IN 46032

Tel: 317.810.3700

(the **data exporter**)

And

YOU

(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 Annex 1 above.

The provisions of these Clauses shall apply mutatis mutandis with regard to data exporter affiliates located outside the European Economic Area and Switzerland.

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 sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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 Annex 1 above 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 sub-processor 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 sub-processor 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 Annex 2 above 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 sub-processor 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 Annex 2 above, and a summary description of the security measures, as well as a copy of any contract for sub-processing 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 sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor 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 Annex 2 above 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 sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Annex 2 above 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 sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor 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 sub-processor 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 sub-processor 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 of 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 sub-processor 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

(a) the data exporter promptly notifying the data importer of a claim; and

(b) the data importer being given the possibility to cooperate with the data exporter in the defense and settlement of the claim.

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 sub-processor, 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 sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, 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

Sub-processing

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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor 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 sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing 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 sub-processing 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 sub-processor 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 sub-processor 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.

ANNEX 4: SWISS MODEL CLAUSES

Standard Contractual Clauses for the Transfer Of Personal Data From the Swiss Confederation To Third Countries (Controller To Processor Transfers)

For the purposes of Article 6, paragraph 2, let. a) of the Swiss Federal Act on Data Protection of 1992 (DPA) for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Schlage Lock Company LLC on behalf of and for the benefit of data exporter affiliate(s) of the Schlage Lock Company LLC that are located in Switzerland, who are each entitled to enforce the Clauses as independent data exporters.

Address: 11819 N. Pennsylvania Street, Carmel, IN 46032

Tel: 317.810.3700

(the data exporter)

And

YOU

(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 and legal entities for the transfer by the data exporter to the data importer of the personal data specified in Annex 1 above.

Clause 1. Definitions

For the purposes of the Clauses:

a) "personal data" shall mean any information relating to an identified or identifiable natural person or legal entity ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

b) "sensitive personal data", "personality profile", "process/processing", "controller", "processor", and "supervisory authority" shall have the same meaning as in the Swiss Federal Act on Data Protection of 19 June 1992 ("DPA"), (whereby the "authority" shall mean the competent data protection authority in the territory in which the data exporter is established);

c) the "data exporter" means the controller who transfers the personal data;

d) 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 6 DPA;

e) 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 its instructions, the terms of these Clauses and the terms of the written subcontract;

f) the "applicable data protection law" means the legislation protecting the fundamental rights and freedoms of individuals and legal entities, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the country in which the data exporter is established;

g) "technical and organizational security measures" means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized 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 sensitive personal data and personality profiles (hereinafter, “special categories of personal data”) where applicable are specified in Annex 1 above 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), and Clause 7, Clause 8(2), 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 Clause 9 to Clause 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 country where the data exporter is established) and does not violate the relevant provisions of that county;

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 organizational security measures specified in Annex 2 above 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, unauthorized 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 Article 6 DPA;

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 Annex 2 above, 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 organizational security measures specified in Annex 2 above 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 unauthorized access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

e) to deal promptly and properly with all enquiries 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 Annex 2 above 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

2. 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.

3. 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.

4. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

5. 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

6. 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 Swiss Confederation.

7. 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

8. 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.

9. 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.

10. 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 country in which the data exporter is established, namely the Swiss Federal Act on Data Protection of 19 June 1992 and its implementing Ordinance of 14 June 1993.

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 Clauses.

Clause 11. Subprocessing

11. 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. 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.

12. 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.

13. 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 country in which the data exporter is established, namely the Swiss Federal Act on Data Protection of 19 June 1992 and its implementing Ordinance of 14 June 1993.

14. 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

15. 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.

16. 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.

ANNEX 5: GERMAN COMPANION AGREEMENT

In addition to the Standard Contractual Clauses (processors), this "Commissioned Data Processing Agreement" shall be in place between the German data controller and the data processor, in order to comply with the requirements of the German Federal Data Protection Act:

Commissioned Data Processing Agreement

between

The German affiliates of Schlage Lock Company LLC (collectively, the "**Controller**");

and

YOU (the "**Processor**");

each also referred to as "**Party"** or together referred to as "**Parties**" of this Agreement.

PREAMBLE

In order to ensure compliance by the Controller with data processing obligations pursuant to the applicable laws, in particular section 11 of the German Federal Data Protection Act, Controller and Processor hereby agree as follows:

1. Subject matter

The Processor shall store and process, on behalf of the Controller, the data, including personal data in the scope and for the purposes detailed in **Annex 1 above** (the personal data contained in **Annex 1** hereinafter "**Personal Data**", the data and Personal Data in **Annex 1** collectively "**Data**"). The Data will be provided by Controller to Processor. The Parties may choose to amend **Annex 1** by way of an amendment agreement to reduce or expand the scope and types of processed data.

2. Instructions of the Controller

2.1. The Processor shall process the Data provided by the Controller solely in accordance with the Controller's instructions and the provisions contained in this Agreement. The Controller in particular may give instructions regarding type, extent and method of the data processing, within the limits of the technology used. The Controller confirms verbal instructions in writing or by email.

2.2. The Controller may instruct the Processor to transfer the Data to third parties, in particular Controller's group companies in countries which may not have an adequate level of data protection in the meaning of EC Directive 95/46/EC. In relation to the Personal Data, the Controller already has or, prior to the instruction, will have in place mechanisms in order to ensure that an adequate level of data protection is safeguarded (in particular by concluding data transfer agreements based on the respective EU-model clauses for data transfers to third-countries).

2.3. If the Processor is of the opinion that an instruction infringes applicable data protection rules, it shall immediately notify the Controller.

3. Obligations of the Processor

3.1. Within Processor's area of responsibility, Processor shall structure Processor's internal corporate organisation to ensure compliance with the specific requirements of the protection of Data. Processor shall take the appropriate technical and organisational measures to adequately protect the Data against misuse and loss in accordance with the requirements of applicable data protection regulations. In relation to Personal Data measures hereunder shall include, but not be limited to,

3.1.1. the prevention of unauthorised persons from gaining access to data processing systems (physical access control),

3.1.2. the prevention of data processing systems from being used without authorisation (logical access control),

3.1.3. ensuring that persons entitled to use a data processing system gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and that, in the course of processing or use and after storage, Data cannot be read, copied, modified or deleted without authorisation (data access control),

3.1.4. ensuring that Personal Data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control),

3.1.5. ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from data processing systems, (entry control),

3.1.6. ensuring that Personal Data processed are processed solely in accordance with the instructions (control of instructions),

3.1.7. ensuring that Personal Data are protected against accidental destruction or loss (availability control),

3.1.8. ensuring that Personal Data collected for different purposes can be processed separately (separation control).

A measure as referred to in section 3.11 to 3.18 above shall be in particular, but shall not be limited to, the use of state-of-the-art encryption technology. An overview of the above-entitled technical and organisational measures is attached as **Annex 2** above.

3.2. Processor shall ensure that any personnel entrusted with processing Personal Data have entered into a suitable confidentiality undertakings to maintain confidentiality of the data. The undertakings shall continue after the termination of the above-entitled activities.

3.3. Processor shall, without undue delay, inform Controller in case of a serious interruption of operations, suspicion of breaches of data protection, and any other irregularity in processing the Data.

3.4. Processor shall, without undue delay, inform Controller on controls/checks and other measures conducted by a data protection authority, unless the Processor is prohibited to do so under statutory law.

3.5. Processor shall conduct regular control checks concerning its compliance with its obligations towards data protection and security hereunder.

3.6. Controller shall retain title as to any carrier media provided to Processor as well as any copies or reproductions thereof. Processor shall store such media safely and protect them against unauthorized access by third parties. Processor shall be obliged to securely delete any test and scrap material based on an instruction issued by Controller on a case-by-case basis. Where Controller so decides, Processor shall hand over such material to Controller or store it on Controller's behalf.

3.7. Processor shall appoint a data protection officer. The Processor shall provide his/her contact information to the Controller for direct support.

4. Responsibility of the Controller

4.1. The Controller remains responsible for the legality of the data processing and the Controller is solely responsible for the protection of the data subject's rights pursuant to the data protection rules. The Controller is also solely responsible for providing adequate information to data subjects about the data processes hereunder and, if necessary, obtaining their consent thereto.

4.2. In case that data subjects assert their rights to information, correction, erasure, blocking or deletion the Controller shall inform data subjects that they may exercise these rights solely vis-à-vis the Controller. Said rights shall not be asserted against the Processor. If a data subject approaches the Processor directly with the request to correct, erase, block or delete his/her Personal Data, Processor shall forward the request to Controller for further instructions.

4.3. The Controller is the owner of the Data and is therefore responsible for the data quality. The Controller holds all rights in relation to the Data.

4.4. Controller shall, upon termination of this Agreement and by way of issuing an instruction, stipulate, within a period of time set by Processor, the measures to return data carrier media or to delete stored Data.

4.5. Any additional costs arising in connection with the return or deletion of Data after the termination shall be borne by Controller.

5. Inspection rights of the Controller

5.1. The Controller is entitled to inspect the technical and organisational measures and the data processing work flows in the Processor's company at regular intervals upon reasonably prior written notice and during regular business hours in order to verify compliance by the Processor with the terms and conditions of this Agreement and in particular with the obligations on technical and organizational measures mentioned in Section 3.1 of this Agreement. For such purpose, Controller may collect voluntary disclosures from Processor.

5.2. Processor shall, upon Controller's written request and within a reasonable period of time, provide Controller with all information necessary for such audit.

6. Subcontractors

6.1. The engagement of subcontractors is governed by the Standard Contractual Clauses.

7. Indemnity and liability

7.1. Either Party shall indemnify, defend and hold harmless the other Party from any claims, demands, losses, damages, costs and/or expenses raised by third parties to the extent that they are attributable to the wilful or grossly negligent misconduct by the Party at fault or its employees or its permitted contractors.

7.2. To the extent permitted by applicable law, neither Party shall be liable to the other Party for compensation of loss of profit and/or loss of goodwill.

8. Term

8.1. This Agreement shall remain in force for the term of the agreement with Processor.

8.2. Each Party's right to terminate this Agreement for reason remains unaffected. Either Party may in particular terminate this Agreement by giving to the other Party written notice if the other Party has breached any of its material obligations under this Agreement and failed to cure such default within a reasonable period of time upon receipt of a respective prior written notice.

9. Miscellaneous

9.1. Amendments to this Agreement shall be made in writing. This also applies to the form requirement in this paragraph.

9.2. Should a provision of this Agreement be or become invalid, the validity of the other provisions of this Agreement shall remain unaffected hereby. The Parties agree that in the place of the invalid provision, a legally permitted provision shall apply which comes closest to what the Parties would have agreed if they had taken the partial invalidity into consideration.

9.3. This Agreement shall exclusively be governed by the laws of the Federal Republic of Germany. Both Parties hereby submit to the exclusive jurisdiction of the courts of Germany for any disputes and proceedings arising out of or in connection with this Agreement.

ANNEX 6: POLAND SECURITY

The following terms under Articles 36 - 39 a of the Polish Act on Personal Data Protection of 29 August 1997 (consolidated text: Journal of Laws of 2014, No 1182) (**"PDPA"**) shall apply to data importers processing personal data subject to PDPA.

1. Scope

Data importer shall store and process, on behalf of data exporter, the personal data subject to the PDPA within the scope and for the purposes as set forth below.

2. Data Security Officer

The data importer may upon its discretion appoint an individual who will act as a data security officer and who will supervise compliance with the security measures. In case of appointment of a data security officer, the data security officer shall: (i) ensure compliance with the PDPA; (ii) supervise implementing and updating data processing documentation; (iii) ensure that authorized persons are familiarized with PDPA; (iv) keep a register of data files.

3. Authorizations to process personal data

The persons who have access to the personal data will have authorizations granted by the data exporter or data importer. The data importer shall keep a register of persons authorized to process the personal data, which should include the first names and surnames of the persons authorized to process the personal data, the date of granting authorization and the date of expiry, the scope of the authorization, and the identification number if the personal data is processed in an IT system.

4. Information security policy

The data importer will implement an information security policy, which will include:

4.1 a list of buildings, premises or parts thereof comprising the area where the personal data is processed;

4.2 a list of data files with an indication of the software used for data processing;

4.3 a description of the structure of the data files and an indication of the contents of particular information fields and connections between them;

4.4 the method of transferring data between particular systems;

4.5 a definition of the technical and organizational measures necessary to ensure the confidentiality, integrity and accountability of the data being processed.

5. Instruction on managing the IT system used for data processing

The data importer will implement a directive or policy on managing the IT system used for data processing, which will include:

5.1 the procedures for granting authorization to process data and for the registration of these authorizations in the IT system, as well as the identity of the person responsible for the aforesaid activities;

5.2 the applied methods and means of authorization and the procedures connected with their management and use;

5.3 the procedures for the initiation, suspension and termination of work by the users of the system;

5.4 the procedures for making back-ups of the data files and programs and software tools used for the data processing;

5.5 the method, place and period of storage of electronic information media containing personal data and the backups referred to in point 5.4 above;

5.6 the method of protecting the IT system against software used for gaining unauthorized access to the IT system;

5.7 the method of implementing the requirement that the IT system secures the storage of records on the recipients of personal data (any person to whom the data is disclosed, except for a data subject, a person authorized to carry out data processing, a data processor and state or territorial authorities) to whom the data have been disclosed and the date and the scope of this disclosure, unless the IT system is used for the processing of personal data contained in an open data file;

5.8 the procedures for performing inspections and for maintaining the systems and information media used for personal data processing.

6. IT system used for data processing

For each person whose personal data is being processed within the IT system, that system should secure the storage of records of:

6.1 the date when the data were registered for the first time in the system;

6.2 the identifier of a user who registers personal data in the system, unless the access to the IT system and personal data being processed within this system is available for one person only;

6.3 the data sources, in cases where the data have not been obtained from the data subject;

6.4 information on the recipients of personal data (any person to whom the data is disclosed, except for a data subject, a person authorized to carry out data processing, a data processor and state or territorial authorities) to whom the data have been disclosed and the date and the scope of this disclosure, unless the IT system is used for the processing of personal data contained in an open data file;

6.5 an objection to the processing of personal data for marketing purposes or an objection to the transfer of the data to another data controller.

The storage of records of the information referred to in points 6.1 and 6.2 shall ensue automatically after the user's confirmation of the data recording.

The IT system used for personal data processing shall provide for the preparation and printing of a report, in an intelligible form, including the information referred to in points 6.1 - 6.5.

The IT system used for personal data processing shall be secured in particular against software used for gaining unauthorized access to the IT system and the loss of data which may be caused by any power supply failure or line interference.

The IT system used for personal data processing shall be secured against any dangers originating from a public network by the implementation of physical and logical security measures protecting them from any unauthorized access. In cases where the logical security measures are applied, these measures shall cover the control of data flow between the IT system of the data importer and the public network and shall control the actions initiating from the public network and the IT system of the data importer.

7. Access controls

7.1 Access control mechanisms

The access control mechanisms shall be applied in the IT system used for personal data processing.

The area where personal data is processed shall be secured against the access of unauthorized persons during the absence in this area of the persons authorized to process personal data.

Any unauthorized person may remain inside the secure area where personal data is processed only with the data exporter's or data importer's consent, or in the presence of a person authorized to process personal data.

If the access to data being processed in the IT system is granted to at least two persons, the following conditions shall be ensured: a separate identifier shall be registered for each user of the IT system and access to the data is available only after entering the identifier and user's authentication.

The identifier of a user who has lost authorization to personal data processing should not be granted to other person.

7.2 Passwords

In cases where passwords are used for user authentication, the passwords shall be changed at least once a month. The passwords shall consist of at least 8 characters, including small and capital letters, numbers and special characters.

7.3 Back-up copies

a) Personal data being processed within the IT system shall be secured by making back-ups of the data files and using data processing software.

b) Back-ups should be stored in the premises, secured against any unauthorized access, change, damage or destruction, and should be deleted as soon as their usefulness ceases.

7.4 Devices, discs and other electronic media containing personal data

Devices, discs and other electronic information media containing personal data:

a) for liquidation – are to be devoid of those data records in the first place, and if this is impossible, the records are to be altered to make them unreadable.

b) to be turned over to any other party unauthorized to process personal data – are to be devoid of the personal data records, thereby making them irretrievable.

c) to be repaired – are to be devoid of those data records, thereby making them irretrievable or are to be repaired under the supervision of a person who has been authorized by the controller.

A person using a laptop computer containing personal data shall take special precautions when transporting it, storing it, or using it outside the secured area where personal data is processed, including cryptographic protection measures.

8. Encryption

The data importer shall apply cryptographic protection measures used for authentication to data that is being transferred within the public network.

ANNEX 7: ITALY SECURITY

The technical and organisational security measures implemented by the data importer as set out are supplemented by the security measures specified in Title V, Articles 31 et seq. implemented by Decree no. 196 dated 30 June 2003.

Minimum Security Measures

Personal data undergoing processing shall be kept and controlled, also in consideration of technological innovations, of their nature and the specific features of the processing, in such a way as to minimise, by means of suitable preventative security measures, the risk of their destruction or loss, whether by accident or not, of unauthorized access to the data or of processing operations that are either unlawful or inconsistent with the purposes for which the data have been collected.
The following technical arrangements shall be implemented by the data controller, data processor – if appointed – and the person(s) in charge of the data processing whenever data are processed without electronic means:

- the persons in charge of the data processing shall be instructed in writing with regard to controlling and keeping, throughout the steps required to perform processing operations, records and documents containing personal data. Within the framework of the regular update, to be performed at least at yearly intervals, of the specifications concerning the scope of the processing operations that are entrusted to the individual persons in charge of the data processing, the list of the persons in charge of the data processing may also be drawn up by homogeneous categories of task and corresponding authorisation profile;
- if records and documents containing sensitive personal data are entrusted to the persons in charge of the data processing for the latter to discharge the relevant tasks, said records and documents shall be kept and controlled by the persons in charge of the data processing until they are returned so as to prevent unauthorized entities from accessing them; they shall be returned once the relevant tasks have been discharged;

- access to archives containing sensitive data shall be controlled. The persons authorized to access said archives for whatever purpose after closing time shall be identified and registered. If an archive is not equipped with electronic devices for access control or is not placed under the surveillance of security staff, the persons accessing said archive shall have to be authorized in advance.

Processing personal data by electronic means shall only be allowed if the following minimum security measures are adopted**:**

Computerised Authentication System

1. persons in charge of the data processing shall be allowed to process personal data by electronic means if they are provided with authentication credentials such as to successfully complete an authentication procedure relating either to a specific processing operation or to a set of processing operations;

2. authentication credentials shall consist in an ID code for the person in charge of the data processing as associated with a secret password that shall only be known to the latter person; alternatively, they shall consist in an authentication device that shall be used and held exclusively by the person in charge of the data processing and may be associated with either an ID code or a password, or else in a biometric feature that relates to the person in charge of the data processing and may be associated with either an ID code or a password;

3. one or more authentication credentials shall be assigned to or associated with each person in charge of the data processing;

4. the instructions provided to the persons in charge of the data processing shall lay down the obligation to take such precautions as may be necessary to ensure that the confidential component(s) in the credentials are kept secret and that the devices used and held exclusively by persons in charge of the data processing are kept with due care;

5. where provided for by the relevant authentication system, a password shall consist of at least eight digits; if this is not allowed by the electronic equipment, a password shall consist of the maximum

permitted number of characters. It shall not contain any item that can be easily related to the person in charge of the data processing and shall be modified by the latter when it is first used as well as at least every six months thereafter. If sensitive data are processed, the password shall be modified at least every three months;

6. an ID code, if used, may not be assigned to another person in charge of the data processing even at a different time;

7. authentication credentials shall be de-activated if they have not been used for at least six months, except for those that have been authorized exclusively for technical management purposes;

8. authentication credentials shall be also de-activated if the person in charge of the data processing is disqualified from accessing personal data;

9. the persons in charge of the data processing shall be instructed to the effect that electronic equipment should not be left unattended and made accessible during processing sessions;

10. where data and electronic equipment may only be accessed by using the confidential component(s) of the authentication credential, appropriate instructions shall be given in advance, in writing, to clearly specify the mechanisms by which the Data Controller can ensure that data or electronic equipment are available in case the person in charge of the data processing is either absent or unavailable for a long time and it is indispensable to carry out certain activities without further delay exclusively for purposes related to system operability and security. In this case, copies of the credentials shall be kept in such a way as to ensure their confidentiality by specifying, in writing, the entities in charge of keeping such credentials. Said entities shall have to inform the person in charge of the data processing, without delay, as to the activities carried out.

Authorisation System

11. where authorisation profiles with different scope have been set out for the persons in charge of the data processing, an authorisation system shall be used;

12. authorisation profiles for each person or homogeneous set of persons in charge of the data processing shall be set out and configured prior to start of the processing in such a way as to only enable access to the data that are necessary to perform processing operations;

13. it shall be regularly verified, at least at yearly intervals, that the prerequisites for retaining the relevant authorisation profiles still apply.

Other Security Measures

14. within the framework of the regular update – to be performed at least at yearly intervals – of the specifications concerning the scope of the processing operations that are entrusted to the individual persons in charge of the data processing as well as to the technicians responsible for management and/or maintenance of electronic equipment, the list of the persons in charge of the data processing may also be drawn up by homogeneous categories of task and corresponding authorisation profile;

15. personal data shall be protected against the risk of intrusion and the effects of computer viruses and other type of malwares by implementing suitable electronic means to be updated at least every six months (i.e., antivirus programs);

16. the regular update of computer programmes as aimed at preventing vulnerability and removing flaws of electronic means shall be carried out at least annually (i.e., firewall programs). If sensitive data are processed, such update shall be carried out at least every six months;

17. organisational and technical instructions shall be issued such as to require at least weekly data back-ups.

Additional Measures Applying to Processing of sensitive data

18. sensitive data shall be protected against unauthorized access by implementing suitable electronic means;

19. organisational and technical instructions shall be issued with regard to keeping and using the removable media on which the data are stored in order to prevent unauthorized access and processing;

20. the removable media containing sensitive data shall be destroyed or made unusable if they are not used; alternatively, they may be re-used by other persons in charge of the data processing who are not authorized to process the same data, if the information previously contained in them is not intelligible and cannot be re-constructed by any technical means;

If either the data or electronic means have been damaged, suitable measures shall be adopted to ensure that data access is restored within a specific deadline, which must be compatible with data subjects' rights and not in excess of seven days.