DATA PROCESSING AGREEMENT (DPA)

This Agreement ("Agreement") is made on the date accepted by the parties ("Effective Date"),

BETWEEN

1. **TRUSTWAVE LIMITED** whose place of business is Westminster Tower, 3 Albert Embankment, London SE1 7SP ("**Trustwave**"); and
2. **PURCHASER AND/OR LICENSEE OF APPLICABLE TRUSTWAVE SERVICES** ("**Customer**").

(together the **"Parties"**)

BACKGROUND

Trustwave is receiving and processing personal data as part of the performance of the services contemplated in the Services Agreement (as defined below). The purpose of this DPA is to ensure the protection and security of personal data processed on behalf of Customer by Trustwave under the Services Agreement in accordance with the General Data Protection Regulation ("**GDPR**") and applicable national data protection laws of the EU/EEA Member States. Customer engages Trustwave as a commissioned processor acting on behalf of Customer as stipulated in Art. 28 GDPR

1. CONSIDERATION

For good and valuable consideration, and in consideration of the sum of £1 (one pound) paid by Trustwave to the Customer, the receipt of which the Customer hereby acknowledges, Trustwave and the Customer agree to the terms of this DPA.

2. DATA PROTECTION

2.1 Definitions

For the purposes of this DPA, the terminology and definitions as used by the GDPR shall apply. In addition to that,

"**Customer Data**" means any personal data or information including *business contact information, name, business address, business telephone and or email,* provided by or on behalf of Customer to Trustwave, any of its subcontractors or affiliates, in connection with the Services Agreement;

"**Data Protection Laws**" means all data protection laws applicable to the Parties, as amended from time to time;

"**Member State**" means a country belonging to the European Union or to the European Economic Area;

"**Services Agreement**" means the Services Agreement entered into by the Parties for the purpose of providing the services;

"**Security Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data processed which affects the Customer Data covered by this DPA.

2.2 Details of the processing and responsibilities of the Customer

The Parties agree and acknowledge that the Customer will be acting as a data controller in respect of the Customer Data processed for the purposes of this DPA. The Customer is responsible that the processing activities relating to Customer Data, as specified in the Services Agreement and this DPA, are lawful, fair and transparent in relation to the data subjects, as set out in **Appendix 1 to the Annex**. The subject matter of the processing is performance of the services under the Services Agreement, the duration of the processing will be for the term of the Services Agreement.

2.3 Instructions

2.3.1 With respect to the Customer Data, Trustwave shall process Customer Data (including the transfer of personal data) only in accordance with Customer´s instructions and in order to perform its obligations under the Services Agreement and this DPA and in accordance with this DPA, and not process any personal data for any other purpose. In addition, Trustwave may process Customer Data where required to do so by applicable law, in which case Trustwave shall notify Customer of this requirement prior to processing unless the applicable law prohibits them from doing so.

2.3.2 This DPA and the Services Agreement are Customer's complete and final instructions to Trustwave for the processing of Customer Data. Customer accepts that the following all amount to instructions by Customer to process Customer Data: (a) processing in accordance with the Services Agreement and applicable Order Form(s); and (b) processing initiated by users of the Services. Any further instructions that go beyond the instructions contained in this DPA or the Services Agreement must be within the subject matter of this DPA and the Services Agreement. If the implementation of such further instruction results in costs for Trustwave, Trustwave shall inform the Customer about such costs with an explanation of the costs before implementing the instruction. Only after the Customer's confirmation to bear such costs for the implementation of the instruction, Trustwave is required to implement such further instruction. The Customer shall give further instructions generally in writing, unless the urgency or other specific circumstances require another (e.g., oral, electronic) form. Instructions in another form than in writing shall be confirmed by the Customer in writing without undue delay. Trustwave may refuse further instructions in case such are technically or commercially not feasible.

2.3.3 Trustwave shall promptly inform Customer if, in its opinion, an instruction from Customer infringes the GDPR or other European Union or Member State data protection provision ("**Challenged Instruction**"); in such event Trustwave is not obliged to follow the Challenged Instruction. If Customer confirms the Challenged Instruction upon Trustwave's information and acknowledges its liability for the Challenged Instruction, Trustwave will implement such Challenged Instruction, unless the Challenged Instruction relates to (i) the implementation of technical and organizational measures or (ii) the engagement of subprocessors.

2.4 Obligations of Trustwave

With respect to the Customer Data, Trustwave is obliged to

2.4.1 ensure that any of its personnel used to process Customer Data on behalf of the Customer have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

2.4.2 implement appropriate technical and organisational measures as specified in **Appendix 2 to the Annex** to protect Customer Data against unauthorised or unlawful processing and accidental destruction or loss and Customer confirms that such are appropriate for its use of the services under the Services Agreement. Trustwave may amend the technical and organizational measures from time to time provided that the amended technical and organizational measures are not less protective as those set out in Appendix 2 to the Annex;

2.4.3 assist Customer through the available technical and organisational measures set forth in Appendix 2 to the Annex, insofar as this is possible, with Customer's obligations to respond to requests relating to the exercise of data subject rights under Data Protection Laws concerning information, access, rectification and erasure, restriction of processing, notification, data portability, objection and automated decision-making, taking into account the nature of the processing and the information available to Trustwave and to the extent that Customer Data is not accessible to Customer through

the services provided under the Services Agreement. To the extent the technical and organizational measures specified in Appendix 2 to the Annex or the set-up of the services under the Services Agreement require changes or amendments, Trustwave will advise Customer on the costs to implement such additional or amended technical and organizational measures. Once Customer has confirmed to bear such costs, Trustwave will implement such additional or amended technical and organizational measures to assist Customer to respond to data subject's requests. Customer is obliged to determine whether or not a data subject has a right to exercise any such data subject rights and to give instructions to Trustwave to what extent the assistance is required;

2.4.4 notify Customer without undue delay after Trustwave becomes aware of a Security Breach as defined herein or by Data Protection Laws relating to the services provided by Trustwave at Trustwave or a sub-processor. In case of a Security Breach, Trustwave will reasonably assist the Customer with the Customer's obligation under Data Protection Laws to inform the data subjects and the supervisory authorities, as applicable, by providing relevant information taking into account the nature of the processing and the information available to Trustwave;

2.4.5 provide reasonable assistance to the Customer (if so required by the Customer) with respect to (i) data protection impact assessments as may be required by Art. 35 GDPR and (ii) prior consultations with the supervisory authority as may be required by Art. 36 GDPR that relates to the services provided by Trustwave to the Customer under the Services Agreement and this DPA taking into account the nature of the processing and the information available to Trustwave;

2.4.6 make available to the Customer available information to support the Customer with respect to its obligation to demonstrate compliance with the obligations laid down in this DPA and in Art. 28 GDPR, in particular with respect to the technical and organizational measures and allow for and contribute to audits, including inspections conducted by Customer or another auditor mandated by Customer. Customer is aware that any in-person on-site audits may significantly disturb Trustwave's business operations and may entail high expenditure in terms of cost and time; it being understood that an on-site audit shall only be permissible where specifically required by applicable law or a competent authority.

The Parties agree that the aforementioned information obligation is met by providing Customer - upon Customer's request and subject to a confidentiality agreement between Customer and Trustwave to its reasonable satisfaction - with a copy of an annual audit report based on (i) a SOC2 Type 2 Report, (ii) a PCI-DSS Attestation of Compliance (AOC) for Products and Core Infrastructure and/or (iii) an ISO 27001 Certificate (covering inter alia the principles security, system availability, and confidentiality) or with similar audit certificates created by a third party ("**Audit Report**").

If additional audit activities are legally required, Customer may request inspections conducted by Customer or another auditor mandated by Customer subject to the execution by such other auditor of a confidentiality agreement with Trustwave to its reasonable satisfaction ("**On-Site Audit**"). Such On-Site Audit is subject to the following conditions: (i) On-Site Audits are limited to the extent processing facilities and personnel of Trustwave are involved in the processing activities covered by this DPA; and (ii) On-Site Audits occur not more often than once annually or as required by applicable data protection law and (iii) should be performed during regular business hours, solely insubstantially disrupting Trustwave's business operations and in accordance with Trustwave's security policies, and after at least fifteen (15) business days prior written notice; (iv) audits are restricted to those portions of information and any logically separated or entirely dedicated systems and technology used for the processing of personal data of Customer and (v) to the extent Trustwave can remotely provide the necessary information to Customer, such exchange of information must be performed remotely unless otherwise expressly required by Data Protection Laws. Customer is obliged to create an audit report summarizing the findings and observations of the On-Site Audit ("**On-Site Audit Report**"). On-Site Audit Reports as well as Audit-Reports are confidential information of Trustwave and shall not be disclosed to third parties unless required by applicable data protection law or subject to Trustwave's prior consent;

2.4.7 transfer Customer Data only to a country outside the European Economic Area which is approved by the European Commission as providing an adequate level of protection for Personal Data, the transfer is made pursuant to European Commission-approved standard contractual clauses for the transfer of personal data (as per Clause 3 below), or other appropriate legal data transfer mechanisms are used;

2.4.8 not disclose Customer Data to any third party save as permitted by this DPA, as required by applicable law or as subsequently directed by Customer. Customer acknowledges and agrees that Trustwave may engage sub-processors to process Customer Data and authorizes the use of sub-processors engaged by Trustwave for the provision of the services under the Services Agreement and this DPA. Trustwave may remove, replace or appoint suitable and reliable sub-processors at its own discretion. Trustwave shall ensure that any sub-processors to whom it transfers Customer Data enter into written agreements with Trustwave requiring that the sub-processor abide by terms no less protective than this DPA.

2.4.9 on expiry or termination of this DPA, upon receipt of a written request of Customer, either delete or return to the Customer such Customer Data which are processed by Trustwave on behalf of the Customer under this DPA, and to not further process the Customer Data, after the end of the provision of services, and delete existing copies, unless applicable law requires Trustwave to retain Customer Data.

3. INTERNATIONAL DATA TRANSFERS

If and to the extent Trustwave is in a third country, the Parties enter into an agreement based on the standard contractual clauses as per Commission Decision 2010/87/EU, attached as Annex to this DPA, which shall apply under this DPA to comply with the requirements under Art. 44 et seq GDPR.

If and to the extent there should be contradictions or inconsistencies between the remainder of this DPA and the Annex to this DPA, the provisions of the Annex to this DPA shall prevail. For the avoidance of doubt, provisions of the remainder of this DPA that merely go beyond the Annex to this DPA without contradicting its terms shall remain valid.

4. GOVERNING LAW AND JURISDICTION

This DPA is governed by the law specified in the Services Agreement and subject to the jurisdiction of the courts specified in that agreement.

Annex to DPA

Standard Contractual Clauses for Processors

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

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 Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the 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 Appendix 2 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 Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a 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 Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

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

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the 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.

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

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the 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 subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the 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.

Appendix 1 - Details of the transfer

Data Exporter
The Data Exporter is [Customer, please insert].

Data Importer
The Data Importer is Trustwave Limited.

Data subjects
The personal data transferred may concern the following categories of data subjects (please specify):

Customer staff, Customer's company or company-related website users, or Customer's end customers.

Categories of data
The personal data transferred concern the following possible categories of data:

Full name, business contact details (e.g. work email address, work phone number), IP address, log in details.

Special categories of data
The personal data transferred concern the following special categories of data:

Not anticipated.

Processing operations
The personal data transferred may be subject to the following basic processing activities:

The Customer Data may be processed by Trustwave Limited, its parent company, and wholly owned subsidiaries in the course of providing cybersecurity and/or payment card industry services to Customer, as defined in the Services Agreement. Trustwave may store, access, analyse, or transfer Customer Data as part of its processing activities as defined in the Services Agreement.

Appendix 2 - Technical and Organizational Security Measures

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organizational security measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c):

Physical Access Control
Measures are to be taken so that unauthorised individuals do not have access to the data processing systems with which personal data is processed.

Measures taken by Data Importer:
☒ Permanently locked doors and windows
☒ Security locks
☒ Use of special security doors and armoured glass
☒ Permanently manned reception (building)
☒ Single access entry control systems
☒ Automated system of access control
☒ ID or chip card readers
☒ Code locks on doors
☒ Monitoring installations (e.g. alarm device, video surveillance)
☒ Logging of visitors
☒ Compulsory wearing of ID cards
☒ Security personnel
☒ Careful selection of cleaning and maintenance personnel
☒ Security Awareness Training

System Access Control
Measures are to be taken in order to prevent unauthorised individuals using the data processing systems and methods.

Measures taken by Data Importer:
☒ Individual allocation of user rights
☒ Authentication by username and password

☒ Minimum requirements for passwords (i.e. at least eight characters, alphanumeric combinations allowing use of special characters, no acceptance of trivial passwords (e.g. 12345), no acceptance of same characters in a row)
☒ Password management (storage of password only as hash, blocking of account after three failed log in attempts, logging of failed log in attempts, presentation of last log in (date, time) to user for self-control; compulsory change of password every three month, no acceptance of same password in a row)
☒ Password request after inactivity
☒ Encryption of data
☒ Virus protection and firewall
☒ Intrusion detection systems
☒ Security Awareness Training

Data Access Control

Measures are to be taken to ensure that the parties authorised to use the data processing methods can only access the personal data which they are entitled to access.

Measures taken by Data Importer:
☒ Access to personal data only on a need-to-know-basis
☒ Development of a role-based authorization concept
☒ Permanent updating of role-based authorization concept
☒ General access rights only for limited number of admins
☒ Logging of access to and copying, modifying and deletion of personal data
☒ Encryption of data
☒ Intrusion detection systems
☒ Secured storage of data carriers
☒ Secure data lines, distribution boxes and sockets
☒ Secure deletion of personal data and destruction of data carriers and recording of deletion and destruction.

Transfer Control
Measures are to be taken which ensure that personal data cannot be read, copied, modified or removed in an unauthorised manner during their electronic transmission, transport or storage on data carriers, and that it is possible to check and ascertain to which recipients the transmission of personal data is provided for by means of data transmission facilities.

Measures taken by Data Importer:
☒ Use of VPN tunnels
☒ Encrypted email communication
☒ Content filter for outgoing data
☒ Firewall
☒ Secure transport containers in case of physical transports
☒ Encryption of mobile data carriers (such as USB sticks or external USB hard drives), laptops, tablets and smartphones
☒ Recording of data transfers

Input Control
Measures are to be taken which ensure that it can subsequently be checked and ascertained whether and by whom personal data has been entered, modified or removed in/from data processing systems.

Measures taken by Data Importer:
☒ Logging of entering, modification and removal of personal data in/from the system
☒ Traceability of entering, modification and removal of personal data by logging usernames (not user groups)
☒ Individual allocation of user rights to enter, modify or remove based on a role-based authorization concept

Job Control
Measures are to be taken which guarantee contract data processing in accordance with instructions.

Measures taken by Data Importer:
☒ Diligent selection of service providers (in particular with respect to IT security)
☒ Conclusion of a commissioned data processing agreement
☒ Written instructions to service provider
☒ Service provider has implemented a data protection contact
☒ Service provider has obligated its employees to comply with data secrecy
☒ Internal audit and continuous review of compliance
☒ Documentation of technical and organizational IT security measures implemented by service provider

Availability Control

Physical and logical measures are to be taken in order to ensure that personal data is protected against accidental destruction or loss.
Measures taken by Data Importer:
☒ Uninterruptible power supply and auxiliary power unit
☒ Backup and recovery systems (such as RAID)
☒ Redundant servers in separate location
☒ Physical backup in separate location
☒ Climate monitoring and control for servers
☒ Fire and smoke detection
☒ Fire extinguishing system
☒ Fire resistant doors
☒ Malware protection
☒ Emergency plan

Separation Control
Measures are to be taken which ensure that data collected for different purposes can be processed separately.
Measures taken by Data Importer:
☒ Physically separated storage on different hardware systems or data carriers
☒ Logical client separation
☒ Defining and attaching processing purposes for data sets
☒ Defining and implementing database access properties
☒ Development of a role-based authorization concept
☒ Separation of test data and live data
☒ Encryption of data sets stored for the same purpose
☒ Separating allocation file from data sets when personal data is alias