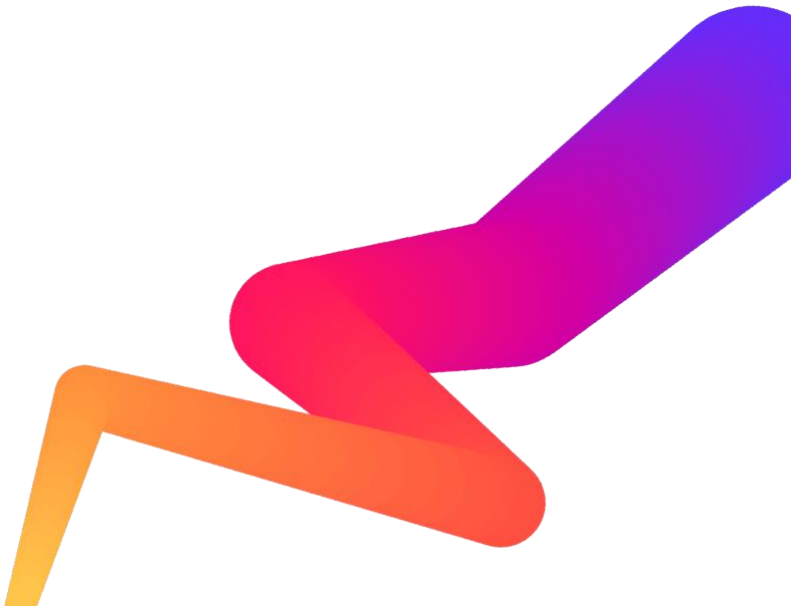
DATA PROCESSING AGREEMENT



DATA PROCESSING AGREEMENT

This data processing agreement is between [●] (the "**Data Processor**") and the Data Controller (as defined below) and incorporates the terms and conditions set out in the Schedules attached hereto (the "**Agreement**").

Each Data Controller has appointed Data Processor to provide services to the Data Controller. As a result of its providing such services to the Data Controller, Data Processor will store and process certain personal information of the Data Controller, in each case as described in further detail in Schedule 2 (*Description of Transfers*).

The Agreement is being put in place to ensure that Data Processor processes Data Controller's personal data on the Data Controller's instructions and in compliance with applicable data privacy laws.

The Parties to this Agreement hereby agree to be bound by the terms and conditions in the attached Schedules as applicable with effect from the date of this Agreement (the "**Effective Date**").

This Agreement may be executed in any number of counterparts, each of which is an original and all of which evidence the same agreement between the parties.

Accepted and agreed to this [●] day of [●] by:

Signature: _____

Name: _____
Date:
On behalf of: [*insert company name; registration number; registered address*]
(the "**Data Processor**")

and by:

Signature: _____

Name: _____
Date
On behalf of: [*insert company name; registration number; registered address*]

("**Data Controller**")

Schedule 1
STANDARD TERMS FOR PROCESSING AGREEMENT

BACKGROUND:

(a) Data Controller wishes to appoint Data Processor to Process Personal Data, as further described in Schedule 2 (*Description of Transfers*).

(b) This Agreement is being put in place to ensure that Data Processor processes Data Controller's Personal Data on Data Controller's instructions and in compliance with the Applicable Data Protection Laws (as defined below).

1. Definitions

1.1 For the purposes of this Agreement, the following expressions bear the following meanings unless the context otherwise requires:

"**Applicable Data Protection Laws**" means (a) the General Data Protection Regulation 2016/679 (the "**GDPR**"); (b) the Privacy and Electronic Communications Directive 2002/58/EC; (c) the UK Data Protection Act 2018 ("**DPA**"), the UK General Data Protection Regulation as defined by the DPA as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, and the Privacy and Electronic Communications Regulations 2003; (d) the California Consumer Privacy Act of 2018 (the "**CCPA**"); and (e) any relevant law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding instrument which implements any of the above or which otherwise relates to data protection, privacy or the use of personal data, in each case as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time;

"**Data Subject**" shall have the meaning given in the relevant Applicable Data Protection Laws;

"**Lawful Export Measure**" means a method allowing for the lawful transfer of Personal Data from a data exporter to a data importer, as may be stipulated by Applicable Data Protection Law or a Regulator from time to time, which may include (depending upon the applicable laws) model transfer terms prescribed by Applicable Data Protection Laws; or prior registration, licensing or permission from a Regulator;

"**Personal Data**" shall have the meaning given in the relevant Applicable Data Protection Laws;

"**Process**", "**Processed**" or "**Processing**" has the meaning given in the relevant Applicable Data Protection Laws;

"**Regulator**" means the data protection supervisory authority which has jurisdiction over a Data Controller's Processing of Personal Data;

"**Standard Contractual Clauses**" means:

(i) in the case of transfers of Personal Data relating to Data Subjects in the European Economic Area ("**EEA**"), the standard contractual clauses for the transfer of Personal Data to data processors established in Third Countries set out in the Commission Decision of 4 June 2021 (C(2021) 3972), as amended and restated from time to time;

(i) in the case of transfers of Personal Data relating to Data Subjects in the United Kingdom, the standard contractual clauses for the transfer of Personal Data to data processors established in Third Countries set out in the Commission Decision of 5 February 2010 (C(2010) 593), as amended and restated from time to time; and

"**Third Country**" means (i) in relation to Personal Data transfers from the EEA, any country outside of the scope of the data protection laws of the EEA, excluding countries approved as providing adequate protection for Personal Data by the European Commission from time to time; (ii) in relation to Personal Data transfers from the UK, any country outside of the scope of the data protection laws of the UK, excluding countries approved as providing

adequate protection for Personal Data by the relevant competent authority of the UK from time to time; and (iii) in relation to Personal Data transfers from any other jurisdiction, any country other than those approved as providing adequate protection for Personal Data by the relevant competent authority of such country from time to time.

2. Conditions of Processing

2.1 This Agreement governs the terms under which Data Processor is required to Process Personal Data on behalf of the Data Controller.

3. Data Processor's Obligations

3.1 Data Processor shall only Process Personal Data on behalf of the Data Controller and in accordance with, and for the purposes set out in the documented instructions received from the Data Controller from time to time and the terms of this Agreement; if it cannot comply with such instructions and/or the terms of the Agreement for whatever reason (including if the instruction violates the Applicable Data Protection Laws), it agrees to inform the Data Controller promptly of its inability to comply, in which case the Data Controller is entitled to suspend the Processing. In no circumstances shall the Data Processor be entitled to Process the Personal Data for its own purposes.

3.2 Data Processor warrants that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the Data Controller and its obligations under this Agreement 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 this Agreement, it will promptly notify the change to the Data Controller as soon as it is aware, in which case the Data Controller are entitled to suspend the transfer and Processing of Personal Data.

3.3 The Data Processor shall grant access to the Personal Data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of this Agreement.

3.4 Data Processor shall ensure that its personnel authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.5 Before Processing Data Controller's Personal Data, Data Processor shall implement, and ensure that its authorised personnel comply with, appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as well as ensuring that those measures continue to provide an appropriate level of security, taking into account the state of the art, the costs of implementation and the nature, scope, context and purpose of the Processing as set out in Schedule 3, or otherwise agreed and documented between the Data Controller and Data Processor from time to time, and shall continue to comply with them during the term of this Agreement. Such measures shall include, as appropriate to the risk:

(i) the pseudonymisation and encryption of Personal Data;

(ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;

(iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

(iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

3.6 Data Processor shall provide data protection and security training to those persons authorised to access the Personal Data and keep a copy of the documentation that evidences the same.

3.7 Data Processor shall promptly notify and assist the Data Controller about any legally binding request for disclosure of Data Controller's Personal Data by a regulatory body, government agency, or law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. The Data Processor shall review the legality of any such request for disclosure and shall challenge the request if it considers there are reasonable grounds to do so; it shall provide the minimum amount of information permissible when responding to such a request. The Data Processor will provide relevant information about disclosure requests to the Data Controller, including in relation to its legality review and any challenges to the request.

3.8 In the event that Data Processor directly receives a request from a Data Subject for access to that Data Subject's Personal Data, or for the rectification or erasure of such Personal Data, or any other request or query from a Data Subject relating to its own Personal Data (including Data Subjects' exercising rights under Applicable Data Protection Laws, such as rights of objection, restriction of processing, data portability or the right not to be subject to automated decision making) (a "**Data Subject Request**"), Data Processor will:

(i) notify the Data Controller immediately of the Data Subject Request (without responding to that Data Subject Request, unless it has been otherwise authorised by the Data Controller to do so);

(ii) provide details of the Data Subject Request (and any other relevant information the Data Controller may reasonably request) to the Data Controller within [3] business days of receipt of Data Subject Request; and

(iii) provide such assistance to the Data Controller as that Data Controller may require for the purposes of responding to the Data Subject Request and to enable that Data Controller to comply with all obligations which arise as a result thereof.

3.9 Data Processor shall deal promptly and properly with all inquiries from Data Controller relating to its Processing of that Data Controller's Personal Data and abide by any specific advice that the Regulator addresses to Data Processor with regard to the Processing of such Personal Data.

3.10 Data Processor shall upon written request from Data Controller from time to time provide that Data Controller with all information necessary to demonstrate Data Processor or Data Controller's compliance with Applicable Data Protection Laws, including of the measures Data Processor has taken to comply with its obligations under this Agreement, and will at its own cost implement any further steps that are necessary to ensure compliance.

3.11 Data Processor shall keep appropriate documentation of the Processing it carries out under this Agreement and shall also inform Data Controller if it becomes aware of any Applicable Data Protection Laws that prevent it from fulfilling its obligations under this Agreement.

3.12 Data Processor shall immediately inform Data Controller if, in its opinion, an instruction infringes Applicable Data Protection Laws.

3.13 [Data Processor shall permit Data Controller at any time upon [seven (7)] days' notice, to be given in writing, to have access to the appropriate part of Data Processor's premises, systems, equipment, and other materials and data Processing facilities to enable the Data Controller (or its designated representative) to inspect or audit the same for the purposes of monitoring compliance with Data Processor's obligations under this Agreement. Such inspection shall:

(i) be carried out by Data Controller or an inspection body composed of independent members and in possession of the required professional qualifications and bound by a duty of confidentiality, selected by the Data Controller, where applicable, in agreement with the Regulator; and

(ii) not relieve Data Processor of any of its obligations under this Agreement.]

3.14 Where:

(i) Data Controller is required to deal or comply with any assessment, enquiry, notice, consultation or investigation by the Regulator; or

(ii) Data Controller is required under the Applicable Data Protection Laws to carry out a data protection impact assessment or consult with the Regulator prior to Processing Personal Data entrusted to the Data Processor under this Agreement,

then Data Processor will co-operate as requested by the Data Controller to enable that Data Controller to comply with all obligations which arise as a result thereof.

3.15 Data Processor shall inform the Data Controller without undue delay if it becomes aware that any of the Personal Data is inaccurate or out of date, and cooperate with the Data Controller to erase or rectify the relevant Personal Data.

3.16 Data Processor shall promptly carry out a request from Data Controller to amend, correct, transfer, block or delete any of the Personal Data necessary to allow that Data Controller to comply with its responsibilities as a data controller.

3.17 Data Processor will not, without the consent of the Data Controller, either:

(i) Process Personal Data in any Third Country; or

(ii) permit any third party including its subcontractors to Process Personal Data in any Third Country.

3.18 To the extent the Data Processor does, with the consent of the Data Controller in accordance with Clause 3.17, Process Personal Data in a Third Country or permit any third party including its subcontractors to Process Personal Data in any Third Country, and it or they are acting as data importer, the Data Processor shall, and shall procure that any of its affiliates, sub-processors, or subcontractors shall (as relevant):

(i) to the extent required by Applicable Data Protection Law:

(A) ensure that such transfer is carried out using a Lawful Export Measure. To the extent such Lawful Export Measure requires (a) a contract imposing appropriate safeguards on the transfer and processing of such Personal Data (which is not otherwise satisfied by this Agreement); (b) a description of the Processing of Personal Data contemplated under this Agreement; and (c) a description of technical and organisational measures to be implemented by the data importer, the parties agree that the Standard Contractual Clauses, the description of processing activities set out in Schedule 2, and the description of technical and organisational measures set out in Schedule 3, shall apply *mutatis mutandis* for the benefit of such transfer, and in relation to any onward transfer of the Personal Data by that data importer to another person, the other person shall comply with the same importer obligations;

(B) in the case of any export outside of the European Union or United Kingdom, comply with the data importer's obligations set out in the Standard Contractual Clauses, which are hereby incorporated into and form part of this Agreement (and the processing details set out in Schedule 2 *(Description of Transfers)* shall apply for the purposes of Annex 1 and the technical and organisational security measures set out in Schedule 3 (*Technical and Organisation Security Measures*) shall apply for the purposes of Annex 2, respectively);

(ii) at Data Controller's request (from time to time), enter separately into the Standard Contractual Clauses with the Data Controller; and

(iii) if agreed between the Data Controller and Data Processor, take any other alternative or additional steps reasonably requested by the Data Controller in order to ensure that such Processing takes place in accordance with the requirements of Applicable Data Protection Laws.

4. Data Breach

4.1 In the event there is, or Data Processor reasonably believes that there is, any improper, unauthorised or unlawful access to, use of, or disclosure of, or any other compromise which affects the availability, integrity or confidentiality of Personal Data which is Processed by Data Processor under or in connection with this Agreement ("**Data Breach**"), then upon becoming aware of such Data Breach, Data Processor shall:

(i) [immediately][without undue delay and at the latest within [●]]after becoming aware of the Data Breach] notify Data Controller in writing of all known details of the Data Breach relating to the Personal Data[, including:

(A) a description of the nature of the Data Breach including, where possible, the categories and approximate number of Data Subjects and records concerned;

(B) the name and contact details of the data protection officer or other contact point where more information can be obtained;

(C) a description of the likely consequences of the Data Breach; and

(D) a description of the measures taken or proposed to be taken to address the Data Breach, including, where appropriate, measures to mitigate its possible adverse effects;]

(ii) provide Data Controller with regular status updates on any Data Breach (including actions taken to resolve the incident) and share additional information related to the breach as soon as more details become available;

(iii) mitigate any harmful effect that is known to Data Processor of a use or disclosure of the Personal Data in violation of this Agreement or in connection with a Data Breach;

(iv) assist Data Controller in remediating or mitigating any potential damage from a Data Breach.

(v) within [4 weeks] of closure of the incident, provide the Data Controller a written report describing the Data Breach, the root cause analysis, actions taken by Data Processor during its response and Data Processor's plans for future actions to prevent a similar Data Breach from occurring;

(vi) not disclose to third parties (including Regulators) any information about a Data Breach involving the Personal Data without prior written and express permission from Data Controller for such disclosure; and

(vii) assist Data Controller with notifying the Data Breach to any Regulator or the Data Subject in accordance with, and in the timeframe required by, the Applicable Data Protection Laws.

5. Changes in Applicable Data Protection Laws

5.1 The parties agree to negotiate in good faith modifications to this Agreement if changes are required for Data Processor to continue to process the Personal Data as contemplated by this Agreement in compliance with the Applicable Data Protection Laws or to address the legal interpretation of the Applicable Data Protection Laws, including (i) to comply with the GDPR or any national legislation implementing it, or the UK General Data Protection Regulation or the DPA, and any guidance on the interpretation of any of their respective provisions; (ii) the Standard Contractual Clauses or any other mechanisms or findings of adequacy are invalidated or amended, or (iii) if changes to the membership status of a country in the European Union or the European Economic Area require such modification.

6. Subcontracting

6.1 Data Processor shall not subcontract to any third party any of its obligations to Process Personal Data on behalf of Data Controller unless all of the following provisions of this clause have first been complied with:

(i) Data Processor has supplied to the Data Controller such information as that Data Controller may require to ascertain that such subcontractor has the ability to comply with Data Processor's obligations set out in this Agreement and with the Data Controller's instructions;

(ii) Data Processor has obtained the prior written consent of the Data Controller;

(iii) the proposed subcontractor has entered into a contract with Data Processor which requires the subcontractor to take adequate technical and organisational measures to safeguard the security and integrity of the relevant Personal Data and only Process data in accordance with the documented instructions of the Data Controller (including as set out in such contract with the proposed subcontractor), and which contains obligations on the relevant subcontractor which are no less onerous than the obligations on the Data Processor in, and which is no less protective of the Personal Data than, the terms of this Agreement. The Data Processor shall provide, at the Data Controller's request, a copy of such subcontractor contract, and subsequent amendments, to the Data Controller.

6.2 In the event that the Data Controller consents to subcontracting the Processing of Personal Data, Data Processor remains liable for the Processing under the terms of this Agreement. The Data Processor shall notify each Data Controller of any failure by a subcontractor to fulfil its obligations under the relevant subcontractor contract.

6.3 The Data Controller hereby consents to the use of the subcontractors set out in Schedule 4 (*Authorised Subcontractors*) for the purposes further described therein, which apply for the purposes of Annex 3 to the Standard Contractual Clauses. If Data Processor intends to make any changes concerning the addition or replacement of the subcontractors set out in Schedule 4 (*Authorised Subcontractors*), it shall comply with the requirements set out in this Clause 6.

7. Confidentiality

(i) Each party (the "**Recipient**") undertakes to the other party (the "**Discloser**") to:

(A) hold all Personal Data of the Discloser which it obtains in relation to this Agreement, in strict confidence;

(B) ensure that employees, agents, officers, consultants, subprocessors, subcontractors, and advisors authorised to Process the Personal Data are subject to binding confidentiality obligations in writing or are under an appropriate statutory obligation of confidentiality and keep a record of the documentation evidencing the same;

(C) not disclose, or authorise the disclosure of, the Discloser's Personal Data to any third party (even after termination of this Agreement) other than pursuant to Clause 6 or as expressly authorised by the other party; and

(D) not to use, or authorise anyone to use, the Discloser's Personal Data for any purpose other than the performance of undertaking the Recipient's obligations or the exercise of its rights or the receipt of any benefits pursuant to this Agreement.

8. Termination

8.1 Termination of this Agreement shall be governed by [*include reference to main services agreement*].

9. Consequences of Termination

9.1 Upon termination of this Agreement:

(i) Data Processor shall, at the Data Controller's option, either forthwith:

(A) return to that Data Controller [or to another data processor designated by the Data Controller] all of the Personal Data and any copies thereof which it is Processing or has Processed upon behalf of that Data Controller. The return of the Personal Data shall result in the full deletion of the Personal Data existent in the IT equipment and systems used by the Data Processor; or

(B) destroy all of the Personal Data and any copies thereof which it has Processed on behalf of that Data Controller promptly and in any case within [14] days of being requested to do so by that Data Controller. The Data Processor shall certify the deletion of such data in writing to the Data Controller; and

(ii) Data Processor shall cease Processing Personal Data on behalf of the Data Controller.

10. Enforcement and Indemnity

10.1 Without prejudice to any other rights or remedies that the Data Controller may have, Data Processor hereby acknowledges and agrees that a person with rights under this Agreement may be irreparably harmed by any breach of its terms and that damages alone may not be an adequate remedy. Accordingly, a person bringing a claim under this Agreement shall be entitled to the remedies of injunction, specific performance or other equitable relief for any threatened or actual breach of the terms of this Agreement.

10.2 Data Processor agrees that it will (in addition to, and without affecting, any other rights or remedies that Data Controller may have whether under statute, common law or otherwise) indemnify and hold harmless Data Controller, on demand from and against all claims, liabilities, costs, expenses, loss or damage incurred by Data Controller (including consequential losses, loss of profit and loss of reputation and all interest, penalties and legal and other professional costs and expenses) arising directly or indirectly from a breach of this Agreement or Applicable Data Protection Laws by Data Processor.

11. Law and Jurisdiction

11.1 This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in all respects in accordance with the laws of [*state country*] and shall be deemed to have been made in [*state country*]. Each party hereby submits to the jurisdiction of the courts of [*state country*].

11.2 Any dispute shall be referred to, and finally resolved by, arbitration administered by the [arbitration centre, e.g. SIAC] in accordance with the [relevant arbitration rules] for the time being in force when the notice of arbitration is submitted. The tribunal shall consist of one arbitrator. The seat of arbitration shall be [country] and the language to be used in the arbitral proceedings shall be English.

Schedule 2
DESCRIPTION OF TRANSFERS

A. LIST OF PARTIES

Data exporter(s) – Data Controller: [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

- Name: [*insert details*]
- Address: [*insert details*]
- Contact person's name, position and contact details: [*insert details*]
- Activities relevant to the data transferred under these Clauses: [*insert details*]
- Role (controller/processor): Controller

Data importer(s) – Data Processor: [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

- Name: [*insert details*]
- Address: [*insert details*]
- Contact person's name, position and contact details: [*insert details*]
- Activities relevant to the data transferred under these Clauses: [*insert details*]
- Role (controller/processor): Processor

B. Description of Transfer

Categories of data subjects whose personal data is transferred

[*To be completed*]

Categories of personal data transferred

[*To be completed*]

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

[*To be completed*]

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

[*To be completed*]

Nature of the processing

[*To be completed*]

Purpose(s) of the data transfer and further processing

[*To be completed*]

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

[*To be completed*]

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

[*To be completed if relevant*]

C. COMPETENT SUPERVISORY AUTHORITY

[*To be completed*]

Schedule 3
TECHNICAL AND ORGANISATION SECURITY MEASURES

Where applicable this Schedule 3 also forms part of the Standard Contractual Clauses.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

[ ]

[1. Physical Access Control

The Data Processor shall take, among others, the following technical and organizational measures in order to establish the identity of the authorized persons and prevent unauthorized access to the Data Processor's premises and facilities in which personal data is processed:

- ☐ All entrances are locked and can only be accessed with the appropriate key / chip card
- ☐ Windows and doors are protected by an alarm system
- ☐ All visitors are required to present identification and are signed in by authorized staff
- ☐ Video monitoring of visitors
- ☐ Visitors are accompanied by Data Processor's personnel at all times
- ☐ Full perimeter and interior surveillance cameras
- ☐ Use of motion detectors to monitor sensitive areas
- ☐ Trained security guards are stationed in and around the building 24x7
- ☐ Co-location facility - separate locked server suites with card readers
- ☐ Other measures: _____

_____

2. System Entry Control

The Data Processor shall take, among others, the following technical and organizational measures in order to prevent unauthorized access to the data processing systems:

- ☐ Unique user authentication via user name and password for each network and system access required (default passwords changed at 1st login)
- ☐ Use of state-of-the-art anti-virus software that includes e-mail filtering and malware detection
- ☐ Use of firewalls
- ☐ During idle times, user and administrator PCs are automatically locked
- ☐ User passwords are changed at least every 90 days and only allow complex passwords

☐ Concept of least privilege, allowing only the necessary access for users to accomplish their job function. Access above these least privileges requires appropriate authorization

☐ Starter, mover & leaver housekeeping processes in place which covers role-based access rights

☐ IT access privileges are reviewed regularly (at least every quarter) by appropriate personnel

☐ RSA 2-factor authentication in place for remote connections

☐ Network monitoring services in place 24 x 7 x 365 to detect unauthorized activities

☐ Vulnerability scanning and remediation in place

☐ Data centre and website penetration testing programme in place

☐ Other measures: _____

_____

3. Data Access Control

The Data Processor shall take, among others, the following technical and organizational measures in order to prevent unauthorized activities in the data processing systems outside the scope of any granted authorizations:

☐ User and administrator access to the network is based on a role based access rights model. There is an authorization concept in place that grants access rights to data only on a "need to know" basis

☐ Administration of user rights through system administrators

☐ Number of administrators is reduced to the absolute minimum

☐ IT governance & controls audits undertaken annually by external 3rd party

☐ Internal control audits undertaken regularly

☐ Network monitoring services in place 24 x 7 x 365 to detect unauthorized activities

☐ Other measures: _____

_____

4. Data Transfer Control

The Data Processor shall take, among others, the following technical and organizational measures in order to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons under their electronic transmission or during their transport or recording on data carriers and to guarantee that it is possible to examine and establish where personal data are or have had to be transmitted by data transmission equipment:

☐ Remote access (including during remote maintenance or service procedures) to the IT systems only via VPN tunnels or other state-of-the-art secure, encrypted connections

☐ Use of e-mail encryption

☐ Data transferred by the Data Processor is transported and saved in encrypted form. The relevant areas of the data carriers are encrypted using data and hard drive encryption software

☐ Data storage devices and paper documents are locked away when not in use (clean desk policy)

☐ Physical transports are only performed with locked containers and/or guarded vehicles

☐ Use of document shredders

☐ Secure destruction processes in place to industry standards utilising specialised 3rd party with disposal certificates produced

☐ The secure transfer modes and encryption methods are regularly updated and kept state-of-the-art (*e.g.*, according to the recommendations in the data protection manual issued by the BSI (Federal Office for Information Security))

☐ 3rd party secure off-site tape storage utilised

☐ Secure communication session established via HTTPS and SFTP protocols across all applications / services

☐ Encrypted certificates utilised for authentication between the web client and the web server across all websites

☐ Other measures: _____

_____

5. Input Control

The Data Processor shall take, among others, the following technical and organizational measures in order to ensure that it is subsequently possible to verify and establish whether and by whom personal data have been entered into data processing systems, altered or removed:

☐ Access to electronic documents / applications is documented via auditable log files

☐ Access to physical documents is documented via protocols

☐ Protocolling input, modification and deletion of data by use of individual user names

☐ Other measures: _____

_____

6. Control of Instructions

The Data Processor shall take, among others, the following technical and organizational measures in order to ensure that personal data which are processed on behalf of Data Controller can only be processed in compliance with Data Controller's instructions:

☐ Clear and binding internal policies contain formalized instructions for data processing procedures

☐ Unambiguous language in the underlying contracts

☐ Careful selection of contractors, especially with regard to data security aspects

☐ Internal monitoring of quality of service includes compliance with contractual arrangements

☐ Regular audits by 3rd parties include compliance with contractual arrangements

☐ Regular staff training to ensure compliance with contractual arrangements and maintain awareness regarding data protection requirements

☐ Secure destruction processes in place to industry standards utilising specialised 3rd party with disposal certificates produced

☐ Periodic risk assessments focus on how insider access is controlled and monitored

☐ The Data Processor's corporate network is separated from its customer services network by means of complex segregation devices

☐ Other measures: _____

_____

7. Availability Control

The Data Processor shall take, among others, the following technical and organizational measures in order to protect the data from accidental destruction or loss:

☐ Appliances for the monitoring of temperature and humidity

☐ Fire / smoke detectors and fire extinguishers in the areas where data is stored / processed

☐ State of the art firewall

☐ Use of state-of-the-art anti-virus software that includes e-mail filtering and malware detection

☐ Data recovery measures and emergency plan in place and regularly tested

☐ Implementation of state-of-the-art backup methods such as: tape backup, data mirroring, and so on. Physical separation of the backup data. Data stored in the archive is saved using redundant systems.

☐ Uses a combination of full, differential, and cumulative backups to ensure data integrity and timely restoration

☐ Backup tapes are securely stored both on-site and off-site to provide protection against disaster and efficient data recovery

☐ To ensure an uninterrupted supply of power to the system, redundant power supply units are built into the systems wherever possible.

☐ Data is stored redundantly on multiple devices

☐ Integrity of stored data regularly verified using checksums

☐ Automated processes move data traffic away from affected area to uncompromised area in case of failure

☐ Preventative maintenance is performed to ensure continued operability of equipment

☐ Other measures: _____

_____

8. Separation and Purpose Control

The Data Processor shall take, among others, the following technical and organizational measures in order to ensure that data collected for different purposes are processed separately:

☐ Documents that are stored physically are stored separately for each customer and the respective containers are clearly labelled

☐ Implementation of an authorization concept

☐ Logical separation of electronically stored customer data (on the software side). Each client has its own designated database for storing information, to ensure that each client’s data is isolated from any other client's data

☐ Strong isolation between guest virtual machines is maintained. Customers are prevented from accessing areas not assigned to them by filtering through the virtualization software.

☐ A unique encryption key is created per customer

☐ Other measures: _____

_____]

Schedule 4
AUTHORISED SUBCONTRACTORS

Subcontractors	**Services provided**	**Description of Processing**	**Contact Details**
[●]	[●]	[●]	Name: Address: Contact Person's: • Name: • Position: • Contact Details:
[●]	[●]	[●]	Name: Address: Contact Person's: • Name: • Position: • Contact Details:
[●]	[●]	[●]	Name: Address: Contact Person's: • Name: • Position: • Contact Details:
[●]	[●]	[●]	Name: Address: Contact Person's: • Name:

			• Position: • Contact Details: