Data Processing Addendum

BETWEEN:

Company

and

tyntec
tyntec Ltd.
20 Farrington Street
London EC4A 4AB
United Kingdom

together the "**Parties**" and each a "**Party**",

as supplemental to the Integration Partner Agreement dated _____ entered into between the Parties (hereinafter referred to as "**the Agreement**"), the Parties wish to execute this Data Processing Addendum which shall be an integral part of the Agreement (the "**Addendum**");

1. DEFINITIONS

For the Purposes of this Addendum:

(a) "**Personal Data**", "**special categories of data**", "**process/processing**", "**controller**", "**processor**", "**data subject**" and "**supervisory authority**" shall have the same meanings given to them in the Regulation (or where the same or similar terms are used under another applicable Data Protection Law, the meanings given to such terms under such Data Protection Law).

(b) "**C-to-P Transfer Clauses**" means the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries approved by EC Commission Decision of 5 February 2010 as set out in Schedule 2 to this Addendum.

(c) "**Data Protection Laws**" means the Regulation, any successor thereto, and any other applicable law relating to the data protection or privacy of individuals.

(d) "**Regulation**" means Regulation (EU) 2016/679 of the European Parliament and the Council (General Data Protection Regulation).

2. ROLE OF THE PARTIES

The Parties agree that Company is the controller and **tyntec** is the processor of all Personal Data processed by **tyntec** on Company's behalf under the Agreement ("**Company Personal Data**"). [The details of the processing activities to be carried out by **tyntec** on behalf of Company are specified in Schedule 1]

3. OBLIGATIONS OF TYNTEC

tyntec warrants and undertakes that:

(a) it will have in place and will maintain appropriate technical and organisational security measures to protect Company Personal Data, which is transferred for the purpose of performing the works and services provided under the Agreement, against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and in particular, where the processing involves the transmission of data over a network, against all other lawful forms of

processing. Having regard to the state of the art and cost of their implementation, tyntec agrees that such measures shall provide a level of security appropriate to the risk represented by the processing and the nature of Company Personal Data to be protected.

(b) it will have in place procedures so that any third party it authorises, to the extent permitted by this Addendum, to have access to Company Personal Data, including its sub-contractors, will respect and maintain the confidentiality and security of Company Personal Data;

(c) it will only collect and process the Company Personal Data specified in Schedule 1 hereto and only on behalf of Company in connection with the Agreement. The collection and the processing of the Company Personal Data by tyntec shall be in accordance with Company's documented instructions and this Addendum and within the scope and for the purposes of the works and services provided under the Agreement, unless otherwise required by European Union or European Member State law to which tyntec is subject;

(d) it will identify to Company a contact point within its organisation authorised to respond to enquiries concerning processing of Company Personal Data and will keep a record of all processing activities carried out on behalf of Company;

(e) it will cooperate in good faith with Company concerning all enquiries regarding the processing of Company Personal Data within a reasonable time.

(f) it will within 48 hours notify Company if it becomes aware of:

(i) any legally binding request for disclosure of Company 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 actual or suspected security breach, accidental or unauthorised access or unlawful processing, misappropriation loss of, damage to or destruction of or other compromise of the security, confidentiality, or integrity of Company Personal Data processed by tyntec or a sub-contractor (**"Security Breach**"); or

(iii) any complaint, communication or request received directly by tyntec or a sub-contractor from a data subject relating specifically to data under the Agreement without responding to that request, unless it has been otherwise authorised to do so by Company, in which case, it shall provide Company with full co-operation and assistance in relation to any such complaint or request and will not respond directly to the data subject without receiving Company's prior written approval to conduct any such direct communication;

(g) upon discovery of any Security Breach, it shall:

(i) immediately take action to prevent any further Security Breach; and

(ii) provide Company with full and prompt cooperation and assistance in relation to any notifications that Company is required to make as a result of the Security Breach;

Notice of any Security Breach shall be made to: _____.

(h) it shall ensure its employees are informed of the confidential nature of Company Personal Data and are obliged to keep such Company Personal Data confidential; have undertaken training relating to handling personal data; and are aware both of tyntec's duties and their personal duties and obligations under this Addendum;

(i) it shall not disclose Company Personal Data whether directly or indirectly to any data subject, person, firm, or other entities without the written consent of Company except to those of its employees who are engaged in the processing of the data and are subject to the binding obligations referred in clause (i) above, to other Company entities at Company's request or as otherwise provided for in this Addendum;

(j) upon Company's and/or data subject's request it shall delete, within 7 days from the receipt of such request, all the Company Personal Data relating to any such specific data subject, and shall provide Company with a written confirmation of the deletion of the aforementioned data, unless it is otherwise required or allowed under law to keep such data.

4. International Data Transfers

(a) No Company Personal Data processed within the European Economic Area (the "**EEA**") by tyntec pursuant to the Agreement shall be exported outside the EEA without adequate safeguards applied by tyntec in accordance with laws.

(b) tyntec agrees to comply with the C-to-P Transfer Clauses in its capacity as the processor whereby Company will be regarded as the Data Exporter and tyntec will be regarded as the Data Importer.

(c) The C-to-P Transfer Clauses may be varied or terminated only as specifically set out in the C-to-P Transfer Clauses.

(d) In the event of inconsistencies between the provisions of the C-to-P Transfer Clauses and this Addendum, the Agreement or other agreements between the Parties, the C-to-P Transfer Clauses shall take precedence. The terms of this Addendum shall not vary the C-to-P Transfer Clauses in any way.

(e) In the event that the C-to-P Transfer Clauses are amended, replaced or repealed by the European Commission or under Data Protection Laws, the Parties shall work together in good faith to enter into any updated version of the C-to-P Transfer Clauses or negotiate in good faith a solution to enable a transfer of Company Personal Data to be conducted in compliance with Data Protection Laws.

5. LIABILITY

(a) The limitation of liability clause included in the Agreement shall apply to this Addendum.

6. SUBCONTRACTING

tyntec shall not subcontract any of its processing operations performed on behalf of Company under the Agreement without the prior written consent of Company. Where tyntec subcontracts its obligations under this Addendum, with the consent of Company, it shall do so only by way of a written agreement with the sub-contractor which imposes the same obligations on the sub-contractor as are imposed on tyntec under this Addendum. Where the sub-contractor fails to fulfil its data protection obligations under such written agreement tyntec shall remain fully liable to Company for the performance of the sub-contractor's obligations under such agreement and upon request it shall promptly send a copy of any agreement it concludes with a sub-contractor under clause 7 below relating to Company Personal Data to Company.

7. ALLOCATION OF COSTS

Notwithstanding anything in contrary in this Addendum, each Party shall perform its obligations under this Addendum at its own cost.

8. TERMINATION

(a) In the event that tyntec is in breach of its obligations under this Addendum, or the Agreement, then Company may temporarily suspend the transfer of Company Personal Data to tyntec until the breach is repaired.

(b) In the event that:

(i) the transfer of Company Personal Data to tyntec has been temporarily suspended for longer than one month pursuant to Clause 10(a);

(ii) compliance by tyntec with this Addendum would put it in breach of its legal or regulatory obligations in the country where tyntec exists;

(iii) Tyntec is in substantial or persistent breach of any warranties or undertakings given by it under this Addendum; or

(iv) a petition is presented for the administration or winding up of tyntec, which petition is not dismissed within the applicable period for such dismissal under applicable laws; a winding up order is made; a receiver is appointed over any of its assets; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs;

then Company, without prejudice to any other rights which it may have against tyntec, shall be entitled to terminate the Agreement and this Addendum.

(c) In the event that the Agreement terminates for any reason, this Addendum shall be immediately terminated.

9. OBLIGATIONS THE TERMINATION IN RESPECT OF PERSONAL DATA PROCESSING SERVICES

The Parties agree that on termination of the data-processing services, tyntec and its sub-contractors, shall, at the choice of Company, return all Company Personal Data and the copies thereof, even if the personal data is anonymized, to Company or shall securely destroy all Company Personal Data and certify to Company that it has done so, unless European Union or Member State legislation imposed upon tyntec and its sub-contractors prevents them from returning or destroying all or part of Company Personal Data. In that case, tyntec warrants that it will guarantee the confidentiality of Company Personal Data and will not actively process Company Personal Data transferred anymore.

IN WITNESS WHEREOF, each Party has caused this Addendum to be executed by its duly authorized representative as of the date first written above.

Company	**tyntec**
Authorized signature:	Authorized signature:
_____	_____
Date:	Date:
Name:	Name:
Title:	Title:

SCHEDULE 1

DETAILS OF THE PROCESSING

The subject-matter of the processing:

Services provided by tyntec as defined in the Agreement

The duration of the processing:

Until the Agreement is terminated

The nature and purpose of the processing:

Processing steps necessary to provide the services defined in the Agreement

The types of personal data:

Data necessary to provide the services defined in the Agreement

The categories of data subjects:

Natural persons and companies

SCHEDULE 2

C-to-P Transfer Clauses

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 of Schedule 2 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 6.2, 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 of Schedule 2;

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 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 Appendix 2 of Schedule 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 sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 of Schedule 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 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 6.1 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 6.1 and 6.2, 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 8.2. 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 Clauses.

CLAUSE 10 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 Clause 6.1 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 11.1 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 11 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 12.1.

APPENDIX 1 OF SCHEDULE 2

DESCRIPTION OF THE TRANSFERS (CONTROLLER TO PROCESSOR)

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

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data Exporter

The Data exporter is Company.

Data Importer

The Data Importer is tyntec.

Data subjects

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

Natural persons and companies

Categories of data

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

Data necessary to provide the services defined in the Agreement.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

N/A

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Processing of data provided by the Controller in order to provide the services defined in the Agreement.

APPENDIX 2 OF SCHEDULE 2

Technical and organisational security measures

This Appendix 2 forms part of the Transfer Clauses and summarizes the technical, organisational and physical security measures implemented by the parties in accordance with Clauses OBLIGATIONS OF THE DATA EXPORTER (d) and OBLIGATIONS OF THE DATA IMPORTER (c) of Schedule 2:

In addition to any data security requirements set forth in the Agreement, the Data Importer shall comply with the following:

Data Importer undertakes to implement, maintain, and continuously control and update, appropriate technical and organizational security measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

This includes:

1. *Preventing unauthorised persons from gaining access to data processing systems with which personal data are processed or used (physical access control); in particular, by taking the following measures:*
    - Controlled access for critical or sensitive areas
    - Video monitoring in critical areas
    - Incident logs
    - Implementation of single entry access control systems,
    - Automated systems of access control,
    - Permanent door and windows locking mechanisms,
    - Key management
    - Permanently manned reception
    - Code locks on doors
    - Monitoring facilities (e.g. alarm device, video surveillance)
    - Logging of visitors
    - Security awareness training

2. *Preventing data processing systems from being used without authorisation (logical access control); in particular, by taking the following measures:*
    - Network devices such as intrusion detection systems, routers and firewalls
    - Secure log-in with unique user-ID/password
    - Policy mandates locking of unattended workstations. Screensaver password is implemented such that if user forgets to lock the workstation, automatic locking is ensured.
    - Logging and analysis of system usage
    - Role-based access for critical systems containing personal data
    - Process for routine system updates for known vulnerabilities
    - Encryption of laptop hard drives
    - Monitoring for security vulnerabilities on critical systems

- Deployment and updating of antivirus software
- individual allocation of user rights, authentication by password and username, minimum requirements for passwords, password management, password request after inactivity, password protection for BIOS, blocking of external ports (such as USB ports), encryption of data, virus protection and use of firewalls, intrusion detection systems.

3. *Ensuring that persons entitled to use a data processing system can gain access only to the data to which they have a right of access, and that, in the course of processing or use and after storage, personal data cannot be read, copied, modified or deleted without authorisation (access control to data); in particular, by taking the following measures:*
    - Network devices such as intrusion detection systems, routers and firewalls
    - Secure log-in with unique user-ID/password
    - Logging and analysis of system usage
    - Role based access for critical systems containing personal data
    - Encryption of laptop hard drives
    - Deployment and updating of antivirus software
    - Definition and management of role based authorization concept, access to personal data only on a need-to-know basis, general access rights only for a limited number of admins, access logging and controls, encryption of data, intrusion detection systems, secured storage of data carriers, secure data lines, distribution boxes and sockets.

4. *Ensuring that personal data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage and that it is possible to verify and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged (data transfer control); in particular, by taking the following measures:*
    - Encryption of communication, tunnelling (VPN = Virtual Private Network), firewall, secure transport containers in case of physical transport, encryption of laptops

5. *Ensuring that it is possible retrospectively to examine and establish whether and by whom personal data have been inserted into data processing systems, modified or removed (entry control); in particular, by taking the following measures:*
    - Logging and analysis of system usage
    - Role based access for critical systems containing personal data
    - Logging and reporting systems, individual allocation of user rights to enter, modify or remove based on role based authorization concept.

6. *Ensuring that personal data processed on the basis of a commissioned processing of personal data are processed solely in accordance with the directions of the data exporter (job control); in particular, by taking the following measures:*
    - Mandatory security and privacy awareness training for all employees
    - Employee hiring procedures which require the completion of a detailed application form for key employees with access to significant personal data and, where allowed by local law
    - Periodic audits are conducted

- Implementation of processes that ensure that Company personal data is only processed as instructed by the data exporter, covering any sub-processors, including diligently selecting appropriate personnel and service providers and monitoring of contract performance, entering into appropriate data processing agreements with sub-processors, which include appropriate technical and organizational security measures.

7. *Ensuring that personal data are protected against accidental destruction or loss (availability control); in particular, by taking the following measures:*
    - Backup procedures and recovery systems, redundant servers in separate location, mirroring of hard disks, uninterruptible power supply and auxiliary power unit, remote storage, climate monitoring and control for servers, fire resistant doors, fire and smoke detection, fire extinguishing system, anti-virus/firewall systems, malware protection, disaster recovery and emergency plan.

8. *Ensuring that data collected for different purposes or different principals can be processed separately (separation control); in particular, by taking the following measures:*
    - Internal client concept and technical logical client data segregation, development of a role based authorization concept, separation of test data and live data.