GENERAL DATA PROCESSING TERMS

WHEREAS

(A) These General Data Processing Terms (**“Terms”**) coupled with a corresponding Data Processing Agreement Specification (**“Specification”**) together constitute a valid Data Processing Agreement (**“DPA”**).

(B) This DPA regulates the protection, safety and confidentiality of the Processing of Personal Data which is shared between the contracting parties for the purposes of executing a Clinical Trial Agreement (**“CTA”**).

(C) The DPA takes effect following the Parties’ signature of a CTA, where such CTA contains the aforementioned Specification, and only when such Specification references these Terms and defines them as applicable. When referring to the DPA and the obligations therein, the Terms and the corresponding Specification cannot be interpreted separately.

(D) The Specification is an integral part or an attachment to the CTA and contains relevant references and details of related Personal Data Processing, as required by these Terms.

(E) The parties to this DPA shall correspond to the CTA, as follows:

1. OPTIMAPHARM d.o.o.

Ulica grada Vukovara 284
HR-10000 Zagreb, Republic of Croatia
EU VAT Number: HR91380434993,

OR an OPTIMAPHARM Local or Branch Office, or a subsidiary of Optimapharm, as defined in the CTA,

as the Contract Research Organization (**“CRO”**) selected by the Sponsor,

2. a research institution, site or hospital (**“Institution”**), and

3. the Principal Investigator (**“PI”**), both contracted by CRO

– individually referred to as **“Party”** and jointly referred to as **“Parties”**.

Therefore the Parties acknowledge and agree to the following DPA provisions:

ART. 1: DEFINITIONS

1.1. For the purposes of this DPA, the following definitions shall apply:

“Data Protection Law”

Shall mean all applicable member state and European Union (EU) law, regulations, bylaws and other requirements regarding Personal Data protection.

“Data Protection Impact Assessment (DPIA)”

Shall mean a privacy impact assessment required by the GDPR before starting certain types of data processing (Art. 35 GDPR),

“GDPR”

Shall mean the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

"Standard Contract Clauses"

Shall mean the standard contractual clauses as set out in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

"Third Country"

Shall mean a country outside the European Economic Area (EEA) except for those for which an adequacy decision was adopted by the European Commission.

1.2. References in this DPA to **"Controller"**, **"Data Subject"**, **"Data Protection Officer"**, **"Personal Data"**, **"Processor"**, **"Processing"**, **"Recipient"** and other such capitalized terms, shall have the same meaning as defined in Art. 4 GDPR.

ART. 2: DATA PROTECTION ROLES

2.1. The Parties acknowledge that regarding the GDPR and Data Protection Law in the context of the CTA their relationships are as follows:

a) the Sponsor is a Controller for a given clinical project,

b) CRO is a Processor of the Sponsor, with delegated and independent contracting responsibilities,

c) the Institution is an independent Controller, and

d) the PI is a Recipient of Personal Data.

2.2. Owning to the unique nature of responsibilities of the Parties in the clinical trial industry, and the independent nature of the Institution, PI and their staff, the Parties agree that the mutual relationship of the CRO and Institution shall be that of two independent Controllers.

ART. 3: SUBJECT MATTER, CATEGORIES OF DATA TO BE PROCESSED AND CATEGORIES OF DATA SUBJECTS, PURPOSES AND MEANS OF PROCESSING

3.1. This DPA regulates the allocation and performance of the obligations of the Parties vis-à-vis Data Subjects pursuant to Art. 12 through 22 GDPR in the context of the Processing of Personal Data related to the CTA and regulates the other data protection rights and obligations that apply in regard to individual Party responsibility.

3.2. The Parties agree that while conducting business activities each Party shall be independently responsible for the purposes and means of Processing Personal Data and shall thus be responsible for the obligations stipulated in Art. 24 GDPR.

3.3. A detailed description of Processing, including the categories of Personal Data to be Processed, categories of Data Subjects and purpose and means of Processing shall be detailed in Schedule 1 to these Terms and in the Specification.

3.4. The Specification shall, inter alia, contain information on the Data Protection Officers contact details, specify use of special categories of data, the frequency of the data exchange if applicable, and a reference to these Terms.

ART. 4: LAWFULNESS OF DATA PROCESSING

4.1. The Parties undertake to comply with all statutory data protection provisions. In particular, they guarantee the lawfulness of the data Processing carried out on the basis of the CTA.

4.2. The PI shall ensure that he/she is acquainted with the Personal Data protection principles and obligations from this DPA and applicable Data Protection Law and in this regard shall be responsible for any personnel of his/her team.

4.3. If the data Processing is based on consent, the Party responsible for the collection of Personal Data undertakes, prior to collecting such data, to obtain a legally valid consent from the persons concerned in accordance with Art. 4(11) and 7 GDPR. The Party responsible for obtaining consent is also responsible for the documentation of the declarations of consent.

ART. 5: FULFILMENT OF THE INFORMATION OBLIGATIONS UNDER ART. 13 AND 14 GDPR

5.1. The Parties undertake to provide the Data Subjects with the information required under Art. 13 or 14 GDPR in a precise, transparent, comprehensible, and easily accessible form.

5.2. Responsibility for providing the information pursuant to Art. 13 or 14 GDPR to the Data Subjects when Personal Data is collected rests with each Party individually.

ART. 6: NOTIFICATION OF THE ESSENTIAL CONTENT OF THE CONTRACT TO DATA SUBJECTS

The Parties shall make the essential content of this DPA on individual data protection responsibilities available to the Data Subjects in a transparent way, either in electronic or written form.

ART. 7: JURISDICTION OVER APPLICATIONS BASED ON ART. 15 TO 22 GDPR

7.1. In accordance with the GDPR, a Data Subject may assert the rights to which they are entitled under Art. 15 through 22 GDPR against either a Controller or a Processor. The Parties undertake to facilitate and enable those rights.

7.2. The Parties shall promptly answer any Data Subject inquires directed to them and, if required, forward such inquires to the competent Party if the Party is not competent to resolve it under this DPA. The competent Party shall acknowledge receipt of the inquiry to the Party which transmitted it.

ART. 8: DEADLINE FOR THE EXECUTION OF APPLICATIONS BASED ON ART. 15 TO 22 GDPR AND PROCEDURE FOR THE EXECUTION OF APPLICATIONS

8.1. For requests based on Art. 15 GDPR, the Parties undertake to provide the Data Subjects with the information to which they are entitled within one month upon request, or within three months if this period is extended on the basis of Art. 12(3) GDPR.

8.2. Requests under Articles 16 to 22 GDPR shall be, to the extent possible, complied with immediately by the respective competent Party.

ART. 9: DUTY TO DOCUMENT AND EXCHANGE INFORMATION

9.1. The Parties undertake to keep and maintain comprehensive documentation to be able to meet their accountability obligations under Art. 5(2) GDPR.

9.2. The Parties shall cooperate and promptly, without undue delay, provide each other with the necessary information from their respective areas of responsibility when required by the other Party for the purposes of facilitating and maintaining compliance with Data Protection Law. Information will be provided upon request by the other Party or automatically and/or unsolicited if one Party considers it necessary to exchange information in a particular case relating to Personal Data protection or Data Subject rights.

9.3. The cooperation from the previous article shall include, but not be limited to assistance with responding to Data Subject requests, performing DPIAs and transfer impact assessments, and responding to Supervisory Authority requests and communications.

ART. 10: RETENTION PERIOD OF DOCUMENTS

10.1. The Parties undertake to retain all documents required to prove compliant data Processing in accordance with Art. 5(2) GDPR while respecting the related legal requirements and the statutory retention periods.

10.2. Upon termination of the CTA/DPA, the statutory retention periods shall continue to apply.

ART. 11: DATA PROTECTION IMPACT ASSESSMENT

The Parties undertake to carry out a Data Protection Impact Assessment (DPIA) for each Processing activity related to Personal Data which is the subject of this DPA for which such assessment is required in accordance with the Art. 35 GDPR.

ART. 12: DATA PROCESSOR

12.1. If it is necessary to engage data Processors to perform data Processing activities related to the CTA, the Parties undertake to conclude a contract with the selected Processor which complies with the requirements of Art. 28 GDPR.

12.2. The Parties shall carry out appropriate due diligence and only engage data Processors who provide sufficient guarantees to implement appropriate technical and organisational measures in accordance with Art. 28(1) GDPR in order to ensure the Processing is in compliant with the GDPR.

ART. 13: TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

13.1. For the cross-border transfers of Personal Data originating from the EEA to a Party located in a Third Country, which are not made pursuant to other approved security measures as provided for under the GDPR, Standard Contractual Clauses shall apply as defined by this DPA.

13.2. Each Party is further responsible for obligating their Third Country Processors, if any, to comply with the applicable from of the Standard Contractual Clauses in all transfers of Personal Data that are the object of this DPA, and which are not undertaken pursuant to other approved security measures as provided for under the GDPR.

13.3. Between the CRO and an Institution/PI located in a Third Country, clauses from paragraph 1 of this article shall apply as follows:

a) module 1 text shall apply, with CRO as the data exporter, and Institution/PI as the data importer(s),

b) clause 7 shall apply, while clause 11 optional text shall not apply,

c) unless otherwise determined in the Specification (D.2), for the purposes of clause 17 and clause 18(b), the law of the Republic of Croatia and the jurisdiction of its courts shall apply,

d) for the purposes of the appendix to the clauses, Schedule 1 of these Terms and the Specification shall be deemed applicable and valid as to the corresponding information required therein,

e) for the purposes of technical and organisational measures including technical and organisational measures to ensure the security of the data from annex II of the appendix, the data importer / Third Country Processor shall implement measures that are at least equivalent to those specified in Schedule 2 of these Terms.

13.4. If the Standard Contractual Clauses are replaced by any further EU decision, the new version of the clauses shall be deemed applicable to the transfer when the previous version expires, and any required details shall be renegotiated by the Parties.

ART. 14: SUPPLEMENTARY MEASURES FOR TRANSFERS

14.1. Apart from the Standard Contractual Clauses themselves, supplementary security measures shall be adopted by the Parties and their Third Country Processors if indicated by the findings of a transfer impact assessment for a Third Country conducted prior to the data transfer. Supplementary measures shall ensure that the obligations contained in the Standard Contractual Clauses are not undermined under the laws of the data importer or Processor's country.

14.2. Such supplementary security measures shall at least obligate the data importer and/or Third Country Processors that they:

a) challenge data disclosure orders in the event that they receive such an order from any third party that aims to compel the disclosure of any Personal Data processed in accordance with this DPA contrary to Data Protection Law, and take all reasonable measures to direct such a third party to demand data directly from a targeted Data Subject,

b) immediately notify the affected Data Subject and the data exporter of such orders, and if prohibited from informing the Data Subject and/or the data exporter, undertake all lawful efforts in order to acquire the right to deviate from such prohibition and convey as much information and as soon as possible to them,

c) undertake all lawful efforts to challenge a data disclosure order based on legal defects under the laws of the requesting country or under any relevant conflicts with applicable EU or Member State law,

d) if, after the previously described steps, they or any of their affiliates still remain compelled to disclose Personal Data, they will disclose only the minimum amount of such data necessary to satisfy the mandatory scope of the data disclosure order,

e) if due to negligence they fail to undertake the above actions, they shall fully indemnify the Data Subject and the data exporter for any material or non-material damage suffered by the Data Subject or the exporter due to the their disclosure of the Data Subject's Personal Data that were transferred in response to the order of a state body or law enforcement body outside the EU/EEA, which violated the data importer's obligation in accordance with Chapter V of the GDPR and this DPA, regardless of all other legal remedies and compensation that the affected Data Subject or the exporter may undertake or receive.

ART. 15: LIABILITY FOR PERSONAL DATA PROTECTION

15.1. The Contracting Parties shall not be jointly liable in their external relations with respect to the Data Subjects pursuant to Art. 82(4) GDPR for any damages caused by processing not in compliance with the GDPR.

15.2. In the internal relations between the Parties, the Parties are only liable for damages which have occurred within their respective area of responsibility.

15.3. Each Party shall, to the extent of its culpability, indemnify the affected Data Subject and/or other Party for any material or non-material damage suffered by the Data Subject and/or the other Party due to the Party's fault which resulted in a breach of the obligations in this DPA. This shall include disclosure(s) of the Data Subject 's Personal Data that were done in response to a data disclosure order of a state or law enforcement body outside the EU/EEA, which violated that Party's obligation in accordance with Data Protection Law, without prejudice to any other legal remedies and/or compensation that the damaged persons may pursue or receive.

ART. 16: INSURANCE COVERAGE

16.1. Unless otherwise specified in the CTA, regarding Personal Data protection the Parties maintain in full force and effect an insurance coverage that is customary for comparably situated companies.

16.2. The insurance policy coverage includes but is not limited to damages following security failure or a data breach, ransom or extortions, costs to engage specialist organisations to minimise any loss of reputation and GDPR fines and defence costs.

ART. 17: DURATION OF THE DPA

The obligations in this DPA are stipulated for the duration of the CTA, and afterwards for a period of 5 years from the moment the CTA is finished, expired, or otherwise terminated. This duration is without prejudice to any residual GDPR obligations which remain even after this deadline.

ART. 18: FINAL PROVISIONS

18.1. If any provision of this DPA is held to be invalid or unenforceable by any judicial or other competent authority, all other provisions will remain in full force and effect and will not in any way be impaired. The parties shall put in place any replacement provisions required to comply with the Data Protection Law.

18.2. Unless otherwise determined in the Specification (D.1), all disputes arising out of or relating to the DPA shall be interpreted, construed and enforced in accordance with the law of Croatia.

18.3. Unless otherwise determined in the Specification (D.1), each Party irrevocably consents to the exclusive jurisdiction of the courts of Croatia over all such disputes and claims under this DPA and all actions to enforce such claims or to recover damages or other relief in connection with such claims under this DPA, except to the extent that the Data Protection Law requires otherwise.

Schedule 1 – description of processing

Categories of Data Subjects	Categories of Personal Data
☒ Project-related personnel of CRO ☒ Healthcare practitioners, including investigators and site staff ☒ Personnel of clients or sponsors ☒ Independent consultants (when applicable)	☒ First and last name, professional title ☒ Business email ☒ Business phone number ☒ Business address ☒ Work history ☒ References ☒ Educational history ☒ Trainings, certifications, and honours ☒ Government Identification Numbers ☒ Contact preferences
☒ Patients or study subjects	☒ First and last name ☒ Government Identification Numbers ☒ Date of Birth ☒ Patient/subject number or unique identifier(s)/pseudonym specific to the research project ☒ Contact preferences

Nature of the processing
Collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Purpose(s) of processing
Performance of CTA specified and related work/research.

Retention criteria or period
For the duration of the CTA. Certain data may be retained longer, when there is independent legitimate interest for such retention, when required by Data Protection Law or when consented to by the Data Subject.

Schedule 2 – technical and organizational measures for restricted transfers

1. INFORMATION SECURITY ORGANIZATION: INFORMATION SECURITY POLICIES AND STANDARDS

The data importer shall maintain a corporate information security organization that will be in charge of managing the data importer's information security policies.

a. The information security organization shall be responsible for:

   i. Performing periodic on-site security risk assessments of (i) data importers' data processing facilities, systems and applications; and (ii) data processing facilities, systems and applications of processing contractors (as data processors) to the extent that the contractors process the data or interact with the processing environments of the data importer or those of the data importer's associates.

   ii. Organize security assessments conducted by an independent third party (such as vulnerability assessment, information security policy assessment, or penetration testing) on an annual basis.

   iii. Advise the executive management, the audit committee of the data importer, and its board of directors on the information security policies of the data importer, potential risks and mitigation plans.

   iv. Adopt and maintain reasonable and appropriate information security policies, procedures and standards that adequately ensure the confidentiality, integrity and availability of data processed by the data importer. Such policies, procedures, and standards will include, without limitation, those designed to protect data processed from remote locations, including employee remote work facilities and locations.

   v. Periodically evaluate and update the information security policies of the data importer, its procedures and standards in order to address new and emerging threats and changes in legal requirements and industry standards.

   vi. Provide management with guidance and support for information security in accordance with business requirements and relevant laws and regulations.

b. The data importer should document a separate dedicated security policy with regard to the processing of personal data. The policy should be approved by management and communicated to all employees and relevant external parties. The security policy should at least refer to: the roles and responsibilities of personnel, the baseline technical and organizational measures adopted for the security of personal data, the data processors or other third parties involved in the processing of personal data. An inventory of specific policies/procedures related to the security of personal data should be created and maintained, based on the general security policy. Roles and responsibilities related to the processing of personal data should be clearly defined and allocated in accordance with the security policy. The personal data processing security policy should be reviewed and revised, if necessary, on a semester basis.

c. Clear appointment of persons in charge of specific security tasks should be performed, including the appointment of a security officer. The security officer should be formally appointed (documented). The tasks and responsibilities of the security officer should also be clearly set and documented.

d. Conflicting duties and areas of responsibility, for example the roles of security officer, security auditor, and DPO, should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of personal data.

2. **HUMAN RESOURCES SECURITY**

a. The data importer should ensure that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the processing of personal data should also be properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns. The data importer should ensure that all employees understand their responsibilities and obligations related to the processing of personal data. Roles and responsibilities should be clearly communicated during the pre-employment and/or induction process. For the above stated purposes, the data importer should have structured and regular yearly training programs for staff, including specific programs for the induction (to data protection matters) of newcomers.

b. Training programs should educate and inform employees, contractors and other external users of the data importers network, systems and applications about (i) information security threats and concerns; (ii) the requirements of the information security policy; and (iii) their responsibilities and obligations in relation to the processing of data, including personal data.

c. The data importer shall equip employees, contractors, and other external users of its network, systems and applications with appropriate tools and equipment to support the implementation of the organizational security policy requirements during its regular operation, including in regard to remote access to the data importer's infrastructure (such as remote work or customer locations).

d. During internal re-organizations or terminations and change of employment, revocation of rights and responsibilities with respective hand over procedures should be clearly defined. This means that the data importer will ensure that employees, contractors and third-party users leave the organization or change roles in an orderly manner, and that access to personal data is removed when employees leave the organization or change position to a position that does not require access to such data.

e. Prior to up taking their duties employees should be asked to review and agree on the security policy of the data importer and sign respective confidentiality and non-disclosure agreements. Employees involved in high-risk processing of personal data should be bound to specific confidentiality clauses (under their employment contract or other legal act).

3. **ASSET/RESOURCE MANAGEMENT**

a. The data importer shall provide appropriate controls to protect the organizational assets that process data, including personal data. In addition, the data importer will maintain an industry standard data classification system designed to ensure that data, including personal data, is protected by an adequate level of protection at all times.

b. The data importer should have a register of the IT resources used for the processing of personal data (hardware, software, and network). The register should include at least the following information: IT resource, type (e.g., server, workstation), location (physical or electronic). A specific person should be assigned the task for maintaining and updating the register (e.g., IT officer).

c. Roles having access to certain resources should be defined and documented.

d. IT resources should be reviewed and updated on annual basis.

4. PHYSICAL AND LOCATION SECURITY

The data importer shall prevent unauthorized physical access, damage, and interference to its premises, and will take measures to prevent the loss, damage, theft or compromise of property, and interference with its data processing activities. All locations where information systems contain data, including personal data, must have approved security systems in place to control and restrict access to such data. This includes implementing the following measures:

a. The physical perimeter of the IT system infrastructure should not be accessible by non-authorized personnel.

b. Clear identification, through appropriate means e.g., ID badges, for all personnel and visitors accessing the premises of the data importer should be established, as appropriate.

c. Secure zones should be defined and be protected by appropriate entry controls. A physical logbook or electronic audit trail of all access should be securely maintained and monitored.

d. Intruder detection systems should be installed in all security zones.

e. Physical barriers should, where applicable, be built to prevent unauthorized physical access.

f. Vacant secure areas should be physically locked and periodically reviewed.

g. An automatic fire suppression system, closed control dedicated air conditioning system and uninterruptible power supply (UPS) should be implemented at the server room.

h. External party support service personnel should be granted restricted access to secure areas.

5. COMMUNICATIONS AND OPERATIONS MANAGEMENT

The data importer will ensure the correct and secure operation of data processing facilities, including the use of appropriate firewall and encryption technology; and, as much as possible, logging and tracking of all data transmissions.

The data importer will implement and maintain an appropriate level of information security and service delivery in accordance with third party service delivery agreements.

6. SERVER, WORKSTATION AND PORTABLE DEVICE SECURITY

a. Users should not be able to deactivate or bypass security settings.

b. Anti-virus applications and detection signatures should be configured on a daily basis.

c. Users should not have privileges to install or activate unauthorized software applications.

d. The system should have session time-outs when the user has not been active for a certain time period.

e. Critical security updates released by the operating system developer should be installed regularly.

f. Mobile and portable device management procedures should be defined and documented establishing clear rules for their proper use. Specific roles and responsibilities regarding mobile and portable device management should be clearly defined.

g. Mobile devices that are allowed to access the information system should be pre-registered and pre-authorized.

h. Mobile devices should be subject to the same levels of access control procedures (to the data processing system) as other terminal equipment.

i. The data importer should be able to remotely erase personal data (related to its processing operation) on a mobile device that has been compromised.

j. Mobile devices should support separation of private and business use of the device through secure software containers.

k. Mobile devices should be physically protected against theft when not in use.

l. Two factor authentication should be implemented for accessing mobile devices.

m. Personal data stored at the mobile device (as part of the data importer's data processing operation) should be encrypted.

n. Full disk encryption should be enabled on the workstation operating system drives.

o. Database and applications servers should be configured to run using a separate account, with minimum OS privileges to function correctly.

p. Database and applications servers should only process the personal data that are actually needed to process in order to achieve its processing purposes.

q. Encryption of workstation and server storage drives should be implemented.

r. Pseudonymization techniques should be applied through separation of data from direct identifiers to avoid linking to data subject without additional information.

7. NETWORK SECURITY MANAGEMENT

The data importer will ensure the protection of all data of the data exporter, including personal data, in its networks (and the networks of its service providers), and will ensure the protection of the supporting infrastructure.

a. The data importer will maintain protection (including antivirus protection) against malicious code.

b. Whenever access is performed through the Internet, communication should be encrypted through cryptographic protocols (TLS/SSL).

c. Remote access to the IT system should in general be avoided. In cases where this is absolutely necessary, it should be performed only under the control and monitoring of a specific person from the organization (e.g., IT administrator/security officer) through pre-defined devices.

d. Wireless access to the IT system should be allowed only for specific users and processes. It should be protected by encryption mechanisms.

e. Traffic to and from the IT system should be monitored and controlled through Firewalls and Intrusion Detection Systems.

f. Access to the IT system should be performed only by pre-authorized devices and terminal equipment using techniques such as MAC filtering or Network Access Control (NAC).

g. Workstations used for the processing of personal data should preferably not be connected to the Internet unless security measures are in place to prevent unauthorized processing, copying and transfer of personal data on store.

h. The network of the information system used to process personal data should be segregated from the other networks of the data importer.

8. <u>**MEDIA HANDLING**</u>

The data importer shall maintain appropriate processes and procedures to prevent unauthorized disclosure, modification, deletion or destruction of assets, and business interruptions. When media need to be disposed of or reused, procedures are implemented to prevent any subsequent retrieval of information stored on them before they are withdrawn from inventory. This includes the following:

a. Shredding of paper and portable media used to store personal data shall be carried out.

b. Multiple passes of software-based overwriting should be performed on all media before being disposed. Following the software erasure, additional hardware-based measures such as degaussing should be performed. Depending on the case, physical destruction should also be considered.

c. If a third party's services are used to securely dispose of media or paper-based records, a service agreement should be in place and a record of destruction of records should be produced as appropriate. In this case it should be considered that the process takes place at the premises of the data importer (and avoid off-site transfer of personal data).

d. It should not be allowed to transfer personal data from workstations to external storage devices (e.g., USB, DVD, external hard drives).

9. EXCHANGE OF INFORMATION

The data importer will maintain data security, including of the personal data and software exchanged within the organization and with any external entity.

10. ELECTRONIC BUSINESS SERVICES

The data importer will implement appropriate measures to ensure the security of e-business services, including mobile devices and their safe use. The data importer will maintain effective monitoring procedures sufficient to detect unauthorized activities in relation to the data.

11. ACCESS CONTROLS

a. The data importer shall maintain appropriate access control procedures to ensure authorized user access and to prevent unauthorized access, theft or loss of data, including personal data, from information systems, including networks, applications and operating systems. An access control system applicable to all users accessing the IT system should be implemented. The system should allow creating, approving, reviewing and deleting user accounts.

b. An access control policy should be detailed and documented. The data importer should determine in this document the appropriate access control rules, access rights and restrictions for specific user roles towards the processes and procedures related to personal data.

c. Specific access control rights should be allocated to each role (involved in the processing of personal data) following the need-to-know principle.

d. Segregation of access control roles (e.g., access request, access authorization, access administration) should be clearly defined and documented.

e. Roles with excessive access rights should be clearly defined and assigned to limited specific members of staff.

f. The use of common user accounts should be avoided. In cases where this is necessary, it should be ensured that all users of the common account have the same roles and responsibilities.

g. An authentication mechanism should be in place, allowing access to the IT system (based on the access control policy and system). As a minimum a username/password combination should be used. Passwords should respect a certain (configurable) level of complexity.

h. The access control system should have the ability to detect and not allow the usage of passwords that do not respect a certain (configurable) level of complexity.

i. A specific password policy should be defined and documented. The policy should include at least password length, complexity, validity period, as well as number of acceptable unsuccessful login attempts.

j. User passwords must be stored in a “hashed” form.

k. Two-factor authentication should be used for accessing systems that process personal data. The authentication factors could be passwords, security tokens, USB sticks with a secret token, biometrics etc.

12. **EVENT LOGGING**

a. Log files should be activated for each system/application used for the processing of personal data. They should include all types of access to data (view, modification, deletion).

b. Log files should be timestamped and adequately protected against tampering and unauthorized access. Clocks should be synchronized to a single reference time source.

c. Actions of the system administrators and system operators, including addition/deletion/change of user rights should be logged.

d. There should be no possibility of deletion or modification of log files content. Access to the log files should also be logged in addition to monitoring for detecting unusual activity.

e. A monitoring system should process the log files and produce reports on the status of the system and notify for potential alerts.

13. **CRYPTOGRAPHIC CONTROL**

The data importer will take appropriate measures to protect the database, including personal data, starting from reading data (data access), copying, modification or deletion by unauthorized persons during the process of updating or transferring of the data. The data importer will take care of data security, confidentiality, authenticity and data integrity, including personal data, whether in the transmission phase or when in storage or use, in particular throughout the process, using reliable methods and cryptographic means that have proven to be the most secure in the industry. The data importer will, in accordance with its capabilities, ensure that cryptographic protocols are changed as necessary to comply with technological developments and new potential threats. Furthermore, the data importer will maintain and manage the encryption keys at all times and will in no case disclose them to third parties, including government authorities or data protection agencies, in accordance with the provisions of the contract.

14. **MANAGEMENT OF TECHNICAL DEFECTS**

a. The data importer will maintain the security of the application software by monitoring and enabling (adopting) a system to manage processes and procedures to reduce the risks posed by misuse and disclosure of technical deficiencies.

b. The data importer will point out the shortcomings of the information system and data security in a timely manner, giving sufficient time for the deficiencies to be corrected and remedied.

15. **INCIDENT MANAGEMENT**

a. The data importer will harmonize appropriate regulations, procedures and acts to prevent accidental, unauthorized or unlawful destruction, alteration, damage, loss or access to personal data, and to insure the availability and integrity of data. An incident response plan with detailed procedures should be defined to ensure effective and orderly response to incidents pertaining personal data. The incidents' response plan should be documented, including a list of possible mitigation actions and clear assignment of roles.

b. Incidents and personal data breaches should be recorded along with details regarding the event and subsequent mitigation actions performed. Personal data breaches should be reported immediately to the management. Notification procedures for the reporting of the breaches to competent authorities and data subjects should be in place, following art. 33 and 34 GDPR.

c. The data importer should establish the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system processing personal data in the event of an incident/personal data breach.

d. Specific personnel with the necessary responsibility, authority and competence to manage business continuity in the event of an incident/personal data breach should be nominated.

16. **<u>BUSINESS PROCESS MANAGEMENT</u>**

a. The organization should make sure that all changes to the IT system are registered and monitored by a specific person (e.g., IT or security officer). Regular monitoring of this process should take place. A detailed and documented change policy should be in place. It should include: a process for introducing changes, the roles/users that have change rights, timelines for introducing changes. The change policy should be regularly updated.

b. The data importer will take all necessary measures to prevent disruption of work processes and protect important business processes from failure of the information system or accidents and make sure to find a way to eliminate the above in a timely manner.

c. A BCP (Business Continuity Plan) should be detailed and documented (following the general security policy). It should include clear actions and assignment of roles. A level of guaranteed service quality should be defined in the BCP for the core business processes that provide for personal data security.

d. The data importer will have in place adequate alternative, back-up facilities to ensure the integrity and accessibility of information and information processing facilities.

17. **<u>DATA BACKUP</u>**

a. Backup and data restore procedures should be defined, documented and clearly linked to roles and responsibilities.

b. Backups should be given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data.

c. Execution of backups should be monitored to ensure completeness.

d. Full backups should be carried out regularly.

e. Backup media should be regularly tested to ensure that they can be relied upon for emergency use.

f. Scheduled incremental backups should be carried out at least on a daily basis.

g. In case a third-party service for back up storage is used, the copy must be encrypted before being transmitted from the data importer.

h. Copies of backups should be encrypted and securely stored offline in different locations.

18. **DATA PROCESSORS**

a. The data importer, as data controller, shall ensure that its subcontractors, as data processors, provide an adequate level of personal data protection, equivalent to the protection prescribed in this contract. For this purpose, formal guidelines and procedures covering the processing of personal data by data processors (contractors/outsourcing) should be defined, documented and agreed between the data importer and the data processor prior to the commencement of the processing activities. These guidelines and procedures should mandatorily establish the same level of personal data security as mandated in the data importer's security policy.

b. Upon finding out of a personal data breach, the data processor shall notify the data importer without undue delay.

c. Formal requirements and obligations should be formally agreed between the data importer and the data processor. The data processor should provide sufficient documented evidence of compliance.

d. The data importer's organization should regularly audit the compliance of the data processor to the agreed level of requirements and obligations.

e. The employees of the data processor who are processing personal data should be subject to specific documented confidentiality/ non-disclosure agreements.