AGREEMENT REGARDING PROCESSING OF DATA

between

Statens Serum Institut
Artillerivej 5
2300 København S
Denmark
(SSI)

Region Hovedstaden
Kongens Vænge 2
3400 Hillerød
Denmark
(REGIONH)

Danmarks Tekniske Universitet
Anker Engelundsvej 1, bygning 101 A
2800 Kongens Lyngby
Denmark
(DTU)

Københavns Universitet
Nørregade 10
1165 København K
Denmark
(UCPH)

Region Sjælland
Alléen 15
4180 Sorø
Denmark
(ZEALCO)

Karolinska Instituttet
Nobels Vag 5
17177 Stockholm
Sweden
(KI)

Lunds Universitet
Paradisgatan 5c
22100 Lund
Sweden
(ULUND)

WITS HEALTH CONSORTIUM PTY LTD
31 Princess of Wales Terrace, Parktown
Johannesburg, 2193
South Africa
(WHC)

Fundacio Institut de Bioenginyeria de Catalunya
Carrer Baldiri Reixac Planta 2A 10-12
08028 Barcelona
Spain
(IBEC-CERCA)

Fundacion Sector Publico Estatal Centro Nacional Investigaciones Oncologicas Carlos III
C. Melchor Fernandez Almagro 3
28029 Madrid
Spain
(FSP CNIO)

(each a "**Party**"; together the "**Parties**"), the Parties

HAVE AGREED on this agreement (the "**Agreement**") in order to meet the requirements of the GDPR[1] and to ensure the protection of the rights of the data subjects.

[1] 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).

Preamble

1.1. The Parties have entered into Consortium Agreement concluded on 28th of June 2022 (the "Consortium Agreement") concerning the project entitled "RESPIRATORY HOST PATHOGEN INTERACTION" (REACT) (the "Project").

1.2. During the course of the Project, the Parties need to process personal data.

1.3. This Agreement regulates the Parties' responsibilities regarding the processing of personal data in the Project.

1.4. All provisions of the Consortium Agreement that are not expressly amended by regulation herein shall follow the regulation in the Consortium Agreement.

1.5. The Parties have agreed to collaboratively carry out the Project in accordance with the Consortium Agreement.

1.6. As part of the Consortium Agreement, the Parties have agreed upon a research protocol containing a series of work packages (the "Protocol").

1.7. The Parties contribute differently with data, know-how and information that is needed to implement actions or exploit results in the work packages.

1.8. The Parties jointly determine the purposes and means of the processing of personal data in the Project as based on the following facts:

- Each Party has participated in the preparatory meetings regarding the organisation of the Project as well as the application for Horizon Europe funding.
- Each Party has had influence on the determination of purpose and means of the processing of personal data within the Project, i.e. the *why* and *how* of the processing.
- The decisions concerning the purpose and means follows from both common decisions and converging decisions as a consequence of the nature of the Project, where each Party contributes differently with data, know-how and information as well as competences to implement actions.

Consequently, the parties

- SSI
- REGIONH
- DTU
- UCPH
- ZEALCO
- KI
- ULUND
- FSP CNIO and
- IBEC-CERCA

are considered joint controllers (each a "**Joint Controller**"; together the "**Joint Controllers**"), cf. GDPR art. 26.

WHC is not part of the European Union and therefore not covered by the GDPR, including art. 26, cf. GDPR art. 3. Furthermore, the contribution from WHC to decisions on *how* of the processing of personal data is to be conducted in the Project has primarily been on an academic level. For both reasons, WHC is not part of the joint controllership. Any processing of personal data by WHC must comply with applicable data protection legislation and standards.

1.9. The prospective collection of biological samples and personal data from medical practices and hospitals and the enclosure of such to the Project is performed by

- REGIONH
- Surveillance Sentinel general practitioners in Denmark and
- Sentinel general practitioners and Hospital departments in Spain

acting as independent data controllers.

The medical practices and hospitals recruit data subjects through their medical practice or hospital and are therefore subject to professional and statutory obligations as doctors, which entails that they are not being able to follow instructions and are obliged to e.g. act against the protocol to secure the safety of the patients. Therefore, they solely determine the purpose and mean of the *actual* processing of personal data in regard to collection of biological samples and personal data directly from the data subjects and the subsequent enclosure of these data to the Project. The independent data controllers are therefore e.g. responsible for finding a legal ground for sharing samples and data, notifying the data subjects according to GDPR art. 13, subject however to Clause 3.3 and 3.4.

1.10. The enclosure of other data, including retrospective cohorts, to the Project is performed by

- SSI
- REGIONH
- KI
- WHC

acting as independent data controllers.

The collection of data was conducted without any linkage to the Project. Therefore, they solely determine the purpose and mean of the processing of personal data in regard to the subsequent enclosure of these data to the Project. The independent data controllers are therefore responsible for e.g. finding a legal ground for sharing data with the project, notifying the data subjects according to GDPR art. 13 (3) and 14 (4) where relevant.

1.11. Consequently, the joint controllership applies to all processing of personal data enclosed to the Project, cf. paragraph 1.6. and 1.7.

1.12. The purpose of this Agreement is to establish and specify the Parties' responsibilities for ensuring compliance with obligations imposed by the applicable GDPR. This Agreement further aims to reflect the Parties' roles and relationships toward the data subjects in a transparent manner and to ensure that the data subjects can exercise their rights in relation to the Parties' processing of personal data. In addition, this Agreement designates a contact point for data subjects exercising their rights under the Project and applicable GDPR. The essence of this agreement will be made available to the data subject on www.react-euproject.eu, cf. GDPR art. 26 (2).

2. Joint controllership and responsibilities

2.1. This Agreement together with the Grant Agreement determines the Joint Controllers' respective responsibilities for compliance with the GDPR and applicable national data protection legislation for the processing of personal data enclosed to the Project, including also data generated in the work packages in the Project, e.g. research results.

2.2. Each Joint Controller is responsible for complying with the GDPR, as well as with any laws applicable to their industry that are generally applicable, when processing personal data within their respective responsibility set out in the Grant Agreement Part A: "List of Work packages" and Part B: "3.2.3 Role of each participant and resources", subject however to Clause 2.4 and 3. This includes that each Joint Controller, within its respective tasks in the project, is responsible for processing, including use, storage and sharing of any personal data and research results is performed in accordance with the principles of the GDPR art. 5, that each Joint Controller shall keep records of the processing within their respective responsibility etc. The personal data may only be processed for scientific or historical research or statistical purposes and may not later be used for any other purposes than scientific or historical research or statistical purposes.

2.3. When possible – bearing the purpose of the processing in mind – the data shall be pseudonymized, in the sense of the GDPR, so that the personal data cannot be attributed to a specific data subject without the use of the link kept separately by the respective providing data controller.

2.4. Sharing of personal data as well as research results in the project shall be performed through the data platform provided by SSI in accordance with the method designated by SSI. SSI is responsible for ensuring that the platform meets the requirements in GDPR, including GDPR art. 32.

2.5. Any personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

This includes e.g. that

- The Joint Controllers shall implement and maintain appropriate technical and organisational measures according to the GDPR, including e.g. art. 5(1)(f), 24, 25 and 32.
- ensure that access to and use of the personal data is limited to individuals specifically designated in the Project and to personnel who require such access to perform the processing of personal data under this Agreement,
- ensure that all of their personnel engaged in the processing of personal data are (i) informed of the confidential nature of the personal data, (ii) have received appropriate training of their responsibilities, (iii) are bound by appropriate confidentiality provisions in accordance with data protection laws and regulations and (iv) are obliged to observe data secrecy. The Joint Controllers shall ensure that such confidentiality obligations survive the termination of their personnel arrangement,
- implement and maintain appropriate technical and organisational measures as set out in Appendix 1. The Joint Controllers understand and agree that these measures are subject to technical progress and development and they are therefore expressly allowed to implement adequate alternative measures as long as the general security described in Appendix 1 is maintained.

2.6. The Joint Controller responsible for a personal data breach, cf. Clause 2.1 shall, without undue delay and, where feasible, no later than seventy-two (72) hours after having become aware of a personal data breach, notify the personal data breach to the supervisory authority competent in accordance with GDPR art. 33 and 55. The Joint Controller responsible for a data breach shall bear all costs associated with the breach.

2.7. Each Joint Controller is under a strict obligation to notify the other Joint Controllers of any personal data breaches without undue delay.

2.8. Each Joint Controller will promptly provide the other Joint Controllers such other information as the Joint Controllers may reasonably request, including, but not limited to documentation of its investigation, provided however that such Joint Controller can legally do so in accordance with applicable laws, rules and regulations, including rules for the protection of public and state security. The Joint Controller responsible for the personal data breach shall be responsible for providing, at its sole expense, any notifications required by GDPR, including notification to the data subjects, provided that the other Joint Controllers is given the opportunity to review and, if legally feasible, approve any breach notification which mentions that Joint Controller. To the extent the Joint Controllers are jointly responsible for a personal data breach, the Joint Controllers agree to work collaboratively to determine the manner of such notification and apportionment of notification costs, considering the relative fault of the Joint Controllers.

2.9. Each Joint Controller shall notify the other joint controllers about significant matters of importance for the joint controllership, e.g. if a Joint Controller considers another Joint Controller to be in violation of the Agreement or applicable GDPR.

3. Data subjects' rights

3.1. According to GDPR art. 26 (3), irrespective of terms of this Arrangement, the data subject may exercise his or her rights under GDPR in respect of and against each of the Joint Controllers. The Joint Controllers have designated several contact points, cf. 3.2., in consideration of the possibility of identifying the person concerned. The contact points will be available to the data subject on www.react-euproject.eu and in the data subject notices, cf. GDPR art. 14.

3.2. Data subjects may use the national appointed contact point with requests, complaints and other queries regarding processing of personal data in the project.

Contact point in Denmark:

Statens Serum Institut
Artillerivej 5
2300 København S

Contact point in Sweden:

Karolinska Instituttet
Nobels Vag 5
17177 Stockholm

Contact Point in Spain:

Fundacion Sector Publico Estatal Centro Nacional Investigaciones Oncologicas Carlos III
C. Melchor Fernandez Almagro 3
28029 Madrid

3.3. Statens Serum Institut is responsible for performing a written notification, cf. art. 14, to the Danish participant in the prospective collection of biological samples and personal data. The notification shall include the relevant point of contact.

3.4. Fundacion Sector Publico Estatal Centro Nacional Investigaciones Oncologicas Carlos III is responsible for performing a written notification, cf. art. 14, to the Spanish participant in the prospective collection of biological samples and personal data. The notification shall include the relevant point of contact.

3.5. Besides Clause 3.3 and 3.4, each Joint Controller shall within their respective responsibility, cf. Clause 2.1, assess whether notification of the data subject is obliged according to the GDPR.

3.6. A Joint Controller who receives a request from a data subject wanting to make use of their rights according to the GDPR, will forward such request to the relevant point of contact, cf. Clause 3.2, who will handle the request initially. The other Joint Controllers will promptly provide such information as the Joint Controller handling the request may reasonably request. The Joint Controllers shall be responsible for providing information, at its sole expense.

3.7. Besides Clause 3.6, the Joint Controller will itself handle inquiries received from data subjects.

3.8. The Joint Controllers agree to work collaboratively to handle any request from a data subject in order to comply with the obligations towards the data subjects.

4. Miscellaneous

4.1. The Joint Controllers understand and agree that they may only transfer personal data to a country outside the EU/EEA ("Third Country") subject to the rules on international transfers of personal data in applicable laws and regulations on data protection, in particular the GDPR.

4.2. This Agreement shall continue to apply for the duration of the processing activities. The Joint Controllers' obligation to ensure that confidentiality applies to personal data continues to apply even after the termination of this Agreement.

5. Damages

5.1. Each Joint Controller shall hold the other joint controllers harmless in respect of any and all loss incurred as a consequence of the Joint Controllers' processing of personal data in contravention of this Agreement or applicable GDPR.

5.2. If a data subject makes a claim for compensation or reimbursement under GDPR art. 82 against one of the Joint Controllers and the claim is legitimately granted, the Joint Controllers shall inter parties have recourse for the costs of compensation or reimbursement to the data subject on the basis of the degree of liability of each Joint Controller for violation of the GDPR, notwithstanding that each Joint Controller may be held liable to the data subjects; in accordance with the principles in GDPR art. 82. Each Joint Controller shall, however, observe the usual time limitation obligation.

5.3. To the extent that one of the Joint Controllers has suffered financial loss as a result of another Joint Controller's failure to comply with the data protection rules, or acts or omissions in this connection, the financial loss may be claimed for compensation or compensation in accordance with the general rules of Danish law.

5.4. Notwithstanding anything else written in this Agreement the Joint Controllers liability against each other shall be limited to direct damages, excluding indirect, special and consequential damages, except for when such damages arise from willful misconduct or gross negligence.

5.5. Each Joint Controller shall carry sufficient insurance as far as it is possible (whether a policy or program of insurance or self-insurance) for a time period sufficient to cover the liability assumed by that Joint Controller hereunder during the term of this Agreement and after.

6. Conflict

6.1. If there is any conflict between any provision of this Agreement and any other arrangement between the Joint Controllers which relates to the processing of personal data, the provisions of this Agreement shall prevail unless the other arrangement is entered into after this Agreement and it is explicitly agreed, in writing, that the other arrangement shall prevail.

7. Term and termination

7.1. This Agreement shall enter into force on the signature date and remain in force until completion of the Project being conducted hereunder and all processing of personal data has been terminated, unless terminated earlier as provided below.

7.2. This Agreement may be terminated by either Joint Controller for any reason by giving the other Joint Controllers thirty (30) days written notice. The termination or expiration of this Agreement does not relieve either Joint Controller of its rights and obligations that have previously accrued.

7.3. For the avoidance of doubt, the obligations of the Joint Controllers with regard to personal data will survive any termination, cancellation, expiration, or other conclusion of this Agreement.

Signatures

Statens Serum Institut

Region Hovedstaden

Danmarks Tekniske Universitet

Københavns Universitet

Region Sjælland

Karolinska Instituttet

Lunds Universitet

WITS HEALTH CONSORTIUM (PTY) LTD

Fundacio Institut de Bioenginyeria de Catalunya

Fundacion Sector Publico Estatal Centro Nacional Investigaciones Oncologicas Carlos III

Appendix 1: Gross list of technical and organizational measures in connection with treatments in the data processor's IT environment

1. Introduction

It is SSI's assessment that the following technical and organizational measures are necessary and appropriate, considering the current technical level, the implementation costs and the nature, scope, context, and purpose of the processing in question, as well as the risks of varying probability and seriousness to the rights and freedoms of natural persons.

2. Field of application

The security requirements in this appendix relate to the processing of personal data. This applies to situations in which SSI acts as data controller, including as part of a joint data responsibility. The requirements must be complied with when SSI processes personal data as data controller. If SSI wishes to make use of data processors to process personal information on SSI's behalf, measures - to the extent that they are relevant - must be submitted to the data processor. In this connection, see SSI's procedure for entering into data processing agreements under j.nr. 22/02752.

3. Technical and organizational security measures

The security level must reflect that the processing includes personal data subject to the data protection regulation's Article 9 on 'special categories of personal data', which is why a 'high' security level should be established.

4. General security requirements

4.1. In order to continuously ensure the security requirements, the principles of a recognized management system for information security management (ISMS) or privacy protection (PIMS) must be followed, for example ISO/IEC 27001, ISO/IEC 27701 or an equivalent (national or international) recognized standard based on a risk management process.

4.2. Processing of personal data must take place in accordance with the minimum technical requirements for state authorities at all times, drawn up by the Digitaliseringsstyrelsen (DIGST) and the Center for Cyber Security (CFCS)2.

4.3. Personal data that is processed must be classified and protected according to internal guidelines and classifications must be in accordance with the management system (e.g., ISMS or PIMS).

4.4. Personal data must, as a rule, be pseudonymised or anonymised in cases where access to specific personally identifiable characteristics is not necessary for the task.

4.5. A record of processing activities in relation to personal data used must be drawn up and maintained.

4.6. There must be ongoing supervision, at least once a year. The supervision must be in accordance with SSI's procedure for supervision of data processors.

[2] Follow the link to the requirements: Sikkerdigital (in Danish).

5. Roles and responsibilities

5.1. Roles and responsibilities in connection with the processing of personal data must be clearly defined and distributed in accordance with the management system used.

5.2. During internal reorganizations or terminations and changes of employment, revocation of rights and responsibilities with respective transfer procedures must be clearly defined.

5.3. There must be a clear appointment of persons responsible for specific security tasks, including the appointment of a security officer.

5.4. The security officer must be formally appointed (documented). The duties and responsibilities of the security officer must also be clearly defined and documented.

5.5. Conflicting responsibilities and duties, for example the roles of the security officer, auditor and DPO, must be considered separate in order to reduce the possibility of unauthorized or accidental change in or misuse of personal data.

6. Ad-hoc workplaces

6.1. Ad-hoc workplaces may only be used if there is a guideline that specifies the requirements regarding confidentiality and appropriate security. This guideline must be available to the data controller at his request.

6.2. 2-factor authentication must be used. The authentication method can e.g., be MitID, SMS token, Rfid or similar.

6.3. When connecting to the internet outside the designated workplace, VPN must be used, and the connection must be encrypted with a minimum of TLS 1.2.

7. Risk mitigation

7.1. The necessary steps must be taken to identify, assess and limit any reasonably foreseeable internal and external risk to the availability, confidentiality and/or integrity of all personal data.

7.2. Identified risks must be reduced to an acceptable level, and the measures used must be documented.

7.3. The above obligation implies that a risk assessment is carried out, and then measures are implemented to address the identified risks. Depending on the relevance of this, the following measures may be involved:

7.4. Pseudonymization and encryption of personal data

7.5. Ability to ensure ongoing confidentiality, integrity, availability and robustness of processing systems and services.

7.6. Ability to promptly restore the availability of and access to personal data in the event of a physical or technical incident.

7.7. A procedure for regular testing, assessment, and evaluation of the effectiveness of the technical and organizational measures to ensure treatment security.

8. Resource and Asset Management

8.1. The organization must ensure that there is a register of the IT resources used for processing personal data (hardware, software, and network). The register must be continuously revised and could at least include the following information: IT resource, type (e.g., server, workstation) and location (physical or electronic). A specific person must be tasked with maintaining and updating the register (e.g., an IT manager).

8.2. Roles that have access to specific resources must be defined and documented.

8.3. IT resources must be reviewed and updated annually.

9. Authorization and access control

9.1. Authorizations must specify the extent to which the user may query, enter, or delete personal data.

9.2. Only the persons authorized to do so may have access to the personal data processed in accordance with the data processing agreement.

9.3. Any processing of personal data must be documented, including which employees have authorization to access the personal data involved.

9.4. Authorized persons must be able to show photo ID during on-site data processing at the data controller.

9.5. Only persons who are employed with the purposes for which the personal data are processed may be authorized. The individual users must not be authorized for uses that they do not need.

9.6. Persons for whom access to the personal data is necessary for auditing or operational and system technical tasks must also be authorized.

9.7. The authorized user is provided with a personal user identification and a personal password, which must be used each time the users gain access to the data processing. Passwords must be changed every six months. Passwords must have a sufficient length and complexity. As a starting point, two-factor authentication is used when accessing systems with sensitive personal data via the Internet or other insecure network. The authentication method can e.g., be MitID, SMS token, Rfid or similar.

9.8. Measures must be taken to ensure that only authorized users can access the personal data to which the person concerned is authorized.

9.9. Restrictions on physical access must be established, and areas where personal data is processed must be effectively separated from areas to which there is general access.

9.10. There must be formal procedures for handling password resets and for other situations where normal logical access control is overridden.

9.11. Checks must be carried out on an ongoing basis and at least once every six months to determine whether users have been granted the access and authorizations they should have. This control can e.g., imply that

statistics are created in the systems about the individual user's use of the system, so that it can be ascertained whether issued accesses and authorizations are still being used.

9.12. Authorizations and access for users must be withdrawn when these are no longer assessed as being necessary.

10. Confidentiality and training

10.1. Any person who processes personal data must receive adequate and continuous training and instruction to ensure that personal data is processed in accordance with the management system and relevant legislation.

10.2. Any person who processes personal data must be subject to a duty of confidentiality either as a result of legislation or through contractual conditions.

11. Control of rejected access attempts and logging

11.1. A record must be made of all rejected access attempts. If no more than five consecutive rejected access attempts with the same user identification are registered within a set period, further attempts from this user identification must be blocked. Access is opened for new attempts after 30 minutes at the earliest.

11.2. Machine registration (logging) must be carried out for all processing of personal data. The log must at least contain information about the time and user, and if possible, also: type of use and indication of the person the information used concerned, or the search criteria used. The log must be kept for six months, after which it must be deleted, unless a longer storage period is determined in accordance with the purpose of the log in order to be able to use it as a tool for use in investigations.

12. Input Material

12.1. Input material may only be used by persons who are engaged in the input. Input material must be stored in such a way that unauthorized persons cannot become familiar with the personal data contained therein.

12.2. When it is no longer necessary to preserve the input data, the data processor must delete or destroy the input data.

12.3. The provision regarding deletion or destruction does not apply if the material is covered by preservation/disposal provisions in accordance with other legislation, or if journalized material is processed according to the general archive provisions on preservation, including handing over archives to the State Archives.

13. Output material

13.1. Output material is covered by the same instructions as input material.

13.2. In addition, output data may only be used by persons who are employed for the purposes for which the processing of the personal data is carried out, as well as in connection with auditing, technical maintenance, operational monitoring, and error correction, etc.

14. Mobile storage media

14.1. Mobile storage media may not be used before this has been agreed in writing with the data controller.

14.2. Mobile storage media with personal data must be labelled and must be stored with sufficiently strong encryption and under supervision or under lock and key when not in use.

14.3. Mobile storage media with personal data may only be handed over to authorized persons for the purpose of auditing or operational and system technical tasks.

14.4. A record must be kept of which mobile storage media are used in connection with the data processing.

14.5. Written instructions must be drawn up for the use and storage of removable mobile storage media.

14.6. In connection with the repair and service of computer equipment containing personal data, as well as the sale and disposal of used data media, the necessary measures must be taken to ensure that the personal data is not accidentally or deliberately destroyed, lost, or degraded, or that the personal data comes to knowledge of unauthorized persons, is misused or is otherwise processed in violation of applicable law.

15. Backups

15.1. The same guidelines apply to backup copies as to all other processing of personal data.

15.2. It must be ensured that systems and personal data are regularly backed up.

15.3. Backups must be stored separately from the server in a non-adjacent room to ensure that these are not lost, e.g., as a result of fire or flood.

15.4. Backup copies must always be stored in a safe manner so that they are not lost.

15.5. Backups should be regularly checked, including that backups are readable and complete.

16. Server / database security

16.1. Database and application servers must be configured to run using a separate account with minimum OS rights to function properly.

16.2. Database and application servers shall only process the personal data that is actually necessary to process in order to achieve its processing purpose.

16.3. Personal data must be encrypted at rest unless this is not technically or economically possible.

16.4. Pseudonymization techniques must be used when separating data from direct identifications to avoid linking to the data subject without additional information.

17. Workstation security

17.1. Users must not be able to disable or bypass security settings.

17.2. Antivirus programs must be configured continuously.

17.3. Users shall not have privileges to install or disable unauthorized software applications.

17.4. The system must have session timeouts when the user has not been active for a certain period.

17.5. Critical security updates released by the operating system provider must be installed regularly.

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

17.7. Workstations used for processing personal data should preferably not be connected to the Internet, unless there are security measures to prevent unauthorized processing, copying and transfer of personal data for storage.

17.8. Full disk encryption must be enabled on the workstation operating system drive.

18. Change Management

18.1. There must be formal procedures to ensure that updates to operating systems, databases, applications, and other software are assessed and implemented within a reasonable time.

18.2. There must be formal procedures for change management to ensure that any change is properly authorised, tested, and approved before implementation. The procedure must be supported by an effective separation of functions or management follow-up to ensure that no single person can implement a change alone.

19. Re-establishment of services

19.1. There must be documented contingency procedures that ensure the re-establishment of services within a reasonable time in the event of operational interruptions.

20. Disposal of equipment

20.1. There must be formal processes to ensure that personal data is effectively deleted before disposal of electronic equipment.

20.2. When disposing of equipment, the procedure must be documented, and this documentation must be available upon request.

21. Physical security

21.1. The physical perimeter of the IT system infrastructure must not be accessible to unauthorized personnel.

21.2. Clear identification in an appropriate way, e.g., ID cards, for all staff and visitors who have access to the organization's premises, are established as needed.

21.3. Secure zones must be defined and protected via appropriate entry controls. A physical logbook or an electronic audit trail of all access must be maintained and monitored in a secure manner.

21.4. Intrusion detection systems must be installed in all security zones.

21.5. Physical barriers must be constructed where appropriate to prevent unauthorized physical access.

21.6. Vacant secure areas must be physically locked and regularly reviewed.

21.7. An automatic fire suppression system, dedicated air conditioning system and uninterruptible power supply (UPS and diesel generator) must be implemented in the server room.

21.8. External party support service personnel should have limited access to secure areas.

22. Business Continuity

22.1. The organization must ensure appropriate continuity and availability in IT systems used to process personal data (in the event of an incident / breach of personal data security).

22.2. An alternative treatment facility must be considered depending on the organization and the acceptable "downtime" for the treatment system.