+45 70 20 31 24
www.auditdata.com
info@auditdata.com

SCHEDULE 5 INFORMATION SECURITY AND DATA PROTECTION

1. INFORMATION SECURITY AND DATA PROTECTION

Auditdata understands the complexities of acting in compliance with local requirements and consequently complies with a range of rigorous certifications across territories as required to deliver consistently high processes quality.

1.1 Information Commissioners Office registered

Auditdata is registered since 03 June 2008 with the United Kingdom ICO – Information Commissioners Office. Registration number: Z1349633. The Data Protection Act 1998 requires every organization that processes personal information to register with the Information Commissioner's Office (ICO) unless they are exempt. Failure to do so is a criminal offence. Entry details are available at the Data Protection Register.

1.2 NHS Assured Commercial Third Party

Auditdata supports its leading market position in Audiology Healthcare Solutions by maintaining the rigorous NHS IGSoC (Information Governance Statement of Compliance) process to gain the official status of being an 'Assured Commercial Third Party' to the NHS.

Auditdata has since 2008 committed to completing annual assessment of performance, utilizing the NHS Information Governance Toolkit and to provide an assurance statement indicating that all key requirements are satisfied and agreeing that this may be audited by the Authority.

1.3 ISO/IEC 27001:2013 Audit and Certification

ISO/IEC 27001:2013 is a broad international information security standard for Information Security Management Systems. The ISO/IEC 27001:2013 certificate validates that Auditdata has implemented the internationally recognized information security controls defined in this standard, including guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization.

Auditdata is committed to annual ISO/IEC 27001:2013 certification of our ISMS – Information Security Management System. Our certificate issued by DNV – Business Assurance. The Auditdata ISO/IEC 27001:2013 Statement of Applicability is available in the appendix. The

+45 70 20 31 24
www.auditdata.com
info@auditdata.com

document includes over 110 security controls, and it maps Auditdata security controls to control objectives contained in Annex A of ISO/IEC 27001:2013.

1.4 ISO 13485:2016 Audit and Certification

Auditdata is committed to annual ISO/IEC 13485:2016 certification of our Quality Management System for Medical Devices. The certificate issued by the TÜV Süd is publicly available.

ISO 13485:2016 is a broad international Quality Management System for Medical Devices standard and represents the requirements for a comprehensive quality management system for the design and manufacture of medical devices. The ISO 13485:2016 certificate validates that Auditdata has implemented the internationally recognized standard and reassures consumers that Auditdata medical products have been tested and certified for safety and performance.

Amongst other initiatives this certification is achieved by ensuring compliance of the product development processes to the IEC 62304 international standard on Software Development Life Cycle for medical device software.

Auditdata employs third-party IT systems to deliver IT services to the Customer. Auditdata can confirm compliance with Customer Code of Connection, which is required by the Customer when it is necessary to implement a direct connection between the Customer and Third-Party IT systems in order to deliver the service required by the Customer. Auditdata Cloud Services are hosted in Azure.

2. DATA PROCESSING AGREEMENT

Data Processing Agreement preamble

2.1 This Data Processing Agreement sets out the rights and obligations that apply to the Data Processor's handling of personal data on behalf of the Data Controller.

2.2 This Agreement has been designed to ensure the Parties' compliance with Article 28, subsection 3 of Regulation 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), which sets out specific requirements for the content of data processing agreements.

2.3 The Data Processor's processing of personal data shall take place for the purposes of fulfilment of the Parties 'product Agreement'.

2.4 In the context of the provision of product agreement, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

2.5 The Data Processing Agreement and the 'Product Agreement' shall be interdependent and cannot be terminated separately. The Data Processing Agreement may however – without termination of the 'Product Agreement' – be replaced by an alternative valid data processing agreement.

+45 70 20 31 24
www.auditdata.com
info@auditdata.com

2.6 This Data Processing Agreement shall take priority over any similar provisions contained in other agreements between the Parties, including the 'Product Agreement'.

2.7 Four appendices are attached to this Data Processing Agreement. The Appendices form an integral part of this Data Processing Agreement.

2.8 Appendix A of the Data Processing Agreement contains details about the processing as well as the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

2.9 Appendix B of the Data Processing Agreement contains the Data Controller's terms and conditions that apply to the Data Processor's use of Sub-Processors and a list of Sub-Processors approved by the Data Controller.

2.10 Appendix C of the Data Processing Agreement contains instructions on the processing that the Data Processor is to perform on behalf of the Data Controller (the subject of the processing), the minimum security measures that are to be implemented and how inspection with the Data Processor and any Sub-Processors is to be performed.

2.11 Appendix D of the Data Processing Agreement contains the Parties' provisions for activities that are not contained in this Data Processing Agreement or the Parties' 'Product Agreement'.

2.12 The Data Processing Agreement and its associated Appendices shall be retained in writing as well as electronically by both Parties.

2.13 This Data Processing Agreement shall not exempt the Data Processor from obligations to which the Data Processor is subject pursuant to the General Data Protection Regulation or other legislation.

3. THE RIGHTS AND OBLIGATIONS OF THE DATA CONTROLLER

3.1 The Data Controller shall be responsible to the outside world (including the data subject) for ensuring that the processing of personal data takes place within the framework of the General Data Protection Regulation (GDPR).

3.2 The Data Controller shall therefore have both the right and obligation to make decisions about the purposes and means of the processing of personal data.

3.3 The Data Controller shall be responsible for ensuring that the processing that the Data Processor is instructed to perform is authorised in law.

4. THE DATA PROCESSOR ACTS ACCORDING TO INSTRUCTIONS

4.1 The Data Processor shall solely be permitted to process personal data on documented instructions from the Data Controller unless processing is required under EU or Member State law to which the Data Processor is subject; in this case, the Data Processor shall inform the Data Controller of this legal requirement prior to processing unless that law prohibits such information on important grounds of public interest, cf. Article 28, subsection 3, para a.

+45 70 20 31 24
www.auditdata.com
info@auditdata.com

4.2 The Data Processor shall immediately inform the Data Controller if instructions in the opinion of the Data Processor contravene the General Data Protection Regulation or data protection provisions contained in other EU or Member State law.

5. CONFIDENTIALITY

5.1 The Data Processor shall ensure that only those persons who are currently authorised to do so are able to access the personal data being processed on behalf of the Data Controller. Access to the data shall therefore without delay be denied if such authorisation is removed or expires.

5.2 Only persons who require access to the personal data in order to fulfil the obligations of the Data Processor to the Data Controller shall be provided with authorisation.

5.3 The Data Processor shall ensure that persons authorised to process personal data on behalf of the Data Controller have undertaken to observe confidentiality or are subject to suitable statutory obligation of confidentiality.

5.4 The Data Processor shall at the request of the Data Controller be able to demonstrate that the employees concerned are subject to the above confidentiality.

6. SECURITY OF PROCESSING

6.1 The Data Processor shall take all the measures required pursuant to Article 32 of the General Data Protection Regulation which stipulates that with consideration for the current level, implementation costs and the nature, scope, context and purposes of processing and the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controller and Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

6.2 The above obligation means that the Data Processor shall perform a risk assessment and thereafter implement measures to counter the identified risk. Depending on their relevance, the measures may include the following:

1. Pseudonymization and encryption of personal data
2. The ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services.
3. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
4. A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6.3 The Data Processor shall in ensuring the above – in all cases – at a minimum implement the level of security and the measures specified in Appendix C to this Data Processing Agreement.

+45 70 20 31 24
www.auditdata.com
info@auditdata.com

6.4 The Parties' possible regulation/agreement on remuneration etc. for the Data Controller's or the Data Processor's subsequent requirement for establishing additional security measures shall be specified in the Parties' 'Product Agreement' or in Appendix D to this Data Processing Agreement.

7. USE OF SUB-PROCESSORS

7.1 The Data Processor shall meet the requirements specified in Article 28, subsection 2 and 4 of the General Data Protection Regulation in order to engage another processor (Sub-Processor).

7.2 The Data Processor shall therefore not engage another processor (Sub-Processor) for the fulfilment of this Data Processing Agreement without the prior specific or general written consent of the Data Controller.

7.3 In the event of general written consent, the Data Processor shall inform the Data Controller of any planned changes with regards to additions to or replacement of other data processors and thereby give the Data Controller the opportunity to object to such changes.

7.4 The Data Controller's requirements for the Data Processor's engagement of other sub-processors shall be specified in Appendix B to this Data Processing Agreement.

7.5 The Data Controller's consent to the engagement of specific sub-processors, if applicable, shall be specified in Appendix B to this Data Processing Agreement.

7.6 When the Data Processor has the Data Controller's authorisation to use a sub-processor, the Data Processor shall ensure that the Sub-Processor is subject to the same data protection obligations as those specified in this Data Processing Agreement on the basis of a contract or other legal document under EU law or the national law of the Member States, in particular providing the necessary guarantees that the Sub-Processor will implement the appropriate technical and organisational measures in such a way that the processing meets the requirements of the General Data Protection Regulation. The Data Processor shall therefore be responsible – on the basis of a sub-processor agreement – for requiring that the sub-processor at least comply with the obligations to which the Data Processor is subject pursuant to the requirements of the General Data Protection Regulation and this Data Processing Agreement and its associated Appendices.

7.7 A copy of such a sub-processor agreement and subsequent amendments shall – at the Data Controller's request – be submitted to the Data Controller who will thereby have the opportunity to ensure that a valid agreement has been entered into between the Data Processor and the Sub-Processor. Commercial terms and conditions, such as pricing, that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the Data Controller.

+45 70 20 31 24
www.auditdata.com
info@auditdata.com

7.8 The Data Processor shall in his agreement with the Sub-Processor include the Data Controller as a third party in the event of the bankruptcy of the Data Processor to enable the Data Controller to assume the Data Processor's rights and invoke these as regards the Sub-Processor, e.g. so that the Data Controller is able to instruct the Sub-Processor to perform the erasure or return of data.

7.9 If the Sub-Processor does not fulfil his data protection obligations, the Data Processor shall remain fully liable to the Data Controller as regards the fulfilment of the obligations of the Sub-Processor.

8. TRANSFER OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

8.1 The Data Processor shall solely be permitted to process personal data on documented instructions from the Data Controller, including as regards transfer (assignment, disclosure and internal use) of personal data to third countries or international organisations, unless processing is required under EU or Member State law to which the Data Processor is subject; in such a case, the Data Processor shall inform the Data Controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest, cf. Article 28, subsection 3, paragraph a.

8.2 Without the instructions or approval of the Data Controller, the Data Processor therefore cannot – within the framework of this Data Processing Agreement:

- Disclose personal data to a data controller in a third country or in an international organization
- Assign the processing of personal data to a sub-processor in a third country
- Have the data processed in another of the Data Processor's divisions located in a third country

8.3 The Data Controller's instructions or approval of the transfer of personal data to a third country, if applicable, shall be set out in Appendix C to this Data Processing Agreement.

9. ASSISTANCE TO THE DATA CONTROLLER

9.1 The Data Processor, taking into account the nature of the processing, shall, as far as possible, assist the Data Controller with appropriate technical and organisational measures, in the fulfilment of the Data Controller's obligations to respond to requests for the exercise of the data subjects' rights pursuant to Chapter 3 of the General Data Protection Regulation. This entails that the Data Processor should as far as possible assist the Data Controller in the Data Controller's compliance with:

5. Notification obligation when collecting personal data from the data subject
6. Notification obligation if personal data have not been obtained from the data subject
7. The right of access by the data subject
8. The right to rectification
9. The right to erasure ('the right to be forgotten')

+45 70 20 31 24
www.auditdata.com
info@auditdata.com

10. The right to restrict processing
11. Notification obligation regarding rectification or erasure of personal data or restriction of processing
12. The right to data portability
13. The right to object
14. The right to object to the result of automated individual decision making, including profiling

9.2 The Data Processor shall assist the Data Controller in ensuring compliance with the Data Controller's obligations pursuant to Articles 32-36 of the General Data Protection Regulation taking into account the nature of the processing and the data made available to the Data Processor, cf. Article 28, subsection 3, para f. This entails that the Data Processor should, considering the nature of the processing, as far as possible assist the Data Controller in the Data Controller's compliance with:

a) The obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk associated with the processing.
b) The obligation to report personal data breaches to the supervisory authority (Danish Data Protection Agency) without undue delay and, if possible, within 72 hours of the Data Controller discovering such breach unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.
c) The obligation – without undue delay - to communicate the personal data breach to the data subject when such breach is likely to result in a high risk to the rights and freedoms of natural persons.
d) The obligation to carry out a data protection impact assessment if a type of processing is likely to result in a high risk to the rights and freedoms of natural persons.
e) The obligation to consult with the supervisory authority (Danish Data Protection Agency) prior to processing if a data protection impact assessment shows that the processing will lead to high risk in the lack of measures taken by the Data Controller to limit risk.

9.3 The Parties' possible regulation/agreement on remuneration etc. for the Data Processor's assistance to the Data Controller shall be specified in the Parties' 'Product Agreement' or in Appendix D to this Data Processing Agreement.

10. NOTIFICATION OF PERSONAL DATA BREACH

10.1 On discovery of personal data breach at the Data Processor's facilities or a sub-processor's facilities, the Data Processor shall without undue delay notify the Data Controller. The Data Processor's notification to the Data Controller shall, if possible, take place within 48 hours after the Data Processor has discovered the breach to enable the Data Controller to comply with his obligation, if applicable, to report the breach to the supervisory authority within 72 hours.

+45 70 20 31 24
www.auditdata.com
info@auditdata.com

10.2 According to clause 9.2., paragraph b, of this Data Processing Agreement, the Data Processor shall – considering the nature of the processing and the data available – assist the Data Controller in the reporting of the breach to the supervisory authority. This may mean that the Data Processor is required to assist in obtaining the information listed below which, pursuant to Article 33, subsection 3 of the General Data Protection Regulation, shall be stated in the Data Controller's report to the supervisory authority:

f) The nature of the personal data breach, including, if possible, the categories and the approximate number of affected data subjects and the categories and the approximate number of affected personal data records
g) Probable consequences of a personal data breach
h) Measures which have been taken or are proposed to manage the personal data breach, including, if applicable, measures to limit its possible damage

11. ERASURE AND RETURN OF DATA

11.1 On termination of the processing services, the Data Processor shall be under obligation, at the Data Controller's discretion, to erase or return all the personal data to the Data Controller and to erase existing copies unless EU law or Member State law requires storage of the personal data.

12. INSPECTION AND AUDIT

12.1 The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with Article 28 of the General Data Protection Regulation and this Data Processing Agreement, and allow for and contribute to audits, including inspections performed by the Data Controller or another auditor mandated by the Data Controller.

12.2 The procedures applicable to the Data Controller's inspection of the Data Processor are specified in Appendix C to this Data Processing Agreement.

12.3 The Data Controller's inspection of sub-processors, if applicable, shall as a rule be performed through the Data Processor. The procedures for such inspection are specified in Appendix C to this Data Processing Agreement.

12.4 The Data Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Data Controller's and Data Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the Data Processor's physical facilities on presentation of appropriate identification.

13. THE PARTIES' AGREEMENT ON OTHER TERMS

13.1 (Separate) terms relating to the consequences of the Parties' breach of this Data Processing Agreement, if applicable, shall be specified in the Parties' 'Product Agreement' or in Appendix D to this Data Processing Agreement.

+45 70 20 31 24
www.auditdata.com
info@auditdata.com

13.2 Regulation of other terms between the Parties shall be specified in the Parties' 'Product Agreement' or in Appendix D to this Data Processing Agreement.

14. COMMENCEMENT AND TERMINATION

14.1 This Data Processing Agreement (DPA) shall become effective on the date of both Parties' signs a product delivery contract (Product Agreement) requiring DPA.

14.2 Both Parties shall be entitled to require this Data Processing Agreement renegotiated if changes to the law or inexpediency of the provisions contained herein should give rise to such renegotiation.

14.3 The Parties' agreement on remuneration, terms etc. in connection with amendments to this Data Processing Agreement, if applicable, shall be specified in the Parties' 'Product Agreement' or in Appendix D to this Data Processing Agreement.

14.4 This Data Processing Agreement may be terminated according to the terms and conditions of termination, incl. notice of termination, specified in the 'Product Agreement'.

14.5 This Data Processing Agreement shall apply for the duration of the processing. Irrespective of the termination of the 'Product Agreement' and/or this Data Processing Agreement, the Data Processing Agreement shall remain in force until the termination of the processing and the erasure of the data by the Data Processor and any sub-processors.

i) Signature

On behalf of the Data Processor

Name: Kent Madsen

Position: CTO

E-Mail: compliance@auditdata.com

15. DATA CONTROLLER AND DATA PROCESSOR CONTACTS/CONTACT POINTS

15.1 The Parties may contact each other using the following contacts/contact points:

j) The Parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

+45 70 20 31 24
www.auditdata.com
info@auditdata.com

APPENDIX A

16. INFORMATION ABOUT THE PROCESSING INFORMATION ABOUT THE PROCESSING

The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is:

Processing of Personally, identifying information (PII) and sensitive personal information (SPI),

Processing activity 1: Auditdata processes the PII and SPI of the Customer for the purpose of ensuring the functionality of the product in question.

This agreement has the purpose of processing:

The Data Processor's processing of PII and SPI data on behalf of the Data Controller shall mainly pertain to (the nature of the processing) The product in question is stated in the Product agreement:

- Auditbase PII data-processing on Auditdata cloud operation server
- Auditbase PII application upgrade/support on customers (data controller) own server
- Auditbase PII application upgrade/support on Auditdata EU secure server (temp storage)

- Manage PII data-processing on Auditdata EU cloud operation server (Microsoft Azure)
- Manage PII application upgrade/support on customers (data controller) own server
- Manage PII application upgrade/support on Auditdata EU secure server (temp storage)

- Strato PII data-processing on Auditdata EU cloud operation server (Microsoft Azure)
- Strato PII application upgrade/support on Auditdata EU secure server

- Listo Screener PII data-processing on Auditdata EU cloud operation server (Microsoft Azure)
- Listo Screener PII application upgrade/support on Auditdata EU secure server

- Analytics PII data-processing on Auditdata EU cloud operation server (Microsoft Azure)
- Analytics PII application upgrade/support on Auditdata EU secure server

The processing includes the following types of personal data about data subjects:

The Personal Data categories may be adjusted from time to time, to the extent that the processing of Personal Data and the purposes thereof continue to fall under the general description.

Data subjects: Persons who are registered in connection with (i) hearing tests, including but limited to hearing impaired patients, and (ii) the provision of other services.

Processing includes the following categories of data subject:

Category: Various Personal Data regarding Data subjects
Category: Health Information (Audiological clinical PII)

+45 70 20 31 24
www.auditdata.com
info@auditdata.com

APPENDIX B

17. TERMS OF THE DATA PROCESSER'S USE OF SUB-PROCESSERS AND LIST OF APPROVED SUB-PROCESSERS

17.1 Terms of the Data Processor's use of sub-processors, if applicable

The Data Processor has the Data Controller's general consent for the engagement of sub-processors. The Data Processor shall, however, inform the Data Controller of any planned changes in-, additions to- or replacement of other data processors and thereby give the Data Controller the opportunity to object to such changes. Such notification shall be submitted to the Data Controller a minimum of 1 months prior to the engagement of sub-processors or amendments coming into force. If the Data Controller should object to the changes, the Data Controller shall notify the Data Processor of this immediately after the receipt of the notification. The Data Controller shall only object if the Data Controller has reasonable and specific grounds for such refusal."

17.2 Approved sub-processors

The Data Controller shall on commencement of this Data Processing Agreement approve the engagement of the following sub-processors:

- Microsoft Azure public cloud (The purpose of engaging Microsoft is to utilize the Microsoft Azure hosting and storage facilities to provide the cloud-based services to Customer)

The Data Controller shall on the commencement of this Data Processing Agreement specifically approve the use of the above sub-processors for the processing described for that party. The Data Processor shall not be entitled – without the Data Controller's explicit written consent – to engage a sub-processor for 'different' processing than the one that has been agreed or have another sub-processor perform the described processing.

+45 70 20 31 24
www.auditdata.com
info@auditdata.com

Appendix C

18. INSTRUCTION PERTAINING TO THE USE OF PERSONAL DATA

The subject of/instruction for the processing
See Appendix A The purpose of the Data Processor's processing of personal data on behalf of the Data Controller.

Security of processing
The processing involves a large volume of personal data which are subject to Article 9 of the General Data Protection Regulation on 'special categories of personal data' which is why a 'high' level of security should be established."
Auditdata has implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. These measures include but are not limited to:

- The pseudonymization and encryption of Personal Data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

18.1 Technical and Organization Measures

General practices. Auditdata has implemented and will maintain for Auditdata Products and Services appropriate technical and organizational measures, internal controls, and information security routines intended to protect Personal Data, as defined in the Agreement, against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as set forth in the subsections below. The Customer is wholly responsible for implementing and maintaining security within any applications or virtual machines that Customer uses with the Auditdata Products and Services.

18.1.1 Domain: organization of information security

Security ownership. Auditdata has appointed a security officer (CIO) responsible for coordinating and monitoring the security rules and procedures. Auditdata is ISO 27001 certified.
Security roles and responsibilities. Auditdata's personnel with access to Customer Data are subject to confidentiality obligations.
Risk management program. Auditdata performed a risk assessment before processing the Personal Data or launching the Auditdata Products or Services.
Auditdata retains its security documents pursuant to its retention requirements after they are no longer in effect.

18.1.2 Domain: Asset management

Asset inventory. Auditdata maintains an inventory of all assets on which Personal Data is stored. Access to the inventories of such media is restricted to Auditdata's personnel authorized by the management authorization process to have such access.

18.1.3 Asset handling

+45 70 20 31 24
www.auditdata.com
info@auditdata.com

Auditdata restricts access to Personal Data. The Customer may implement encryption of Personal Data within its application.

Auditdata imposes restrictions on printing Personal Data and has procedures for disposing of printed materials that contain Personal Data.

Auditdata's personnel must obtain its authorization prior to storing Personal Data on portable devices, remotely accessing Personal Data, or processing Personal Data outside its facilities. This includes removing media (e.g., USB sticks and CD ROMs) and documents containing Personal Data from Auditdata's facilities.

18.1.4 Domain: Human resources security

Security training. Auditdata informs its personnel about relevant security procedures and their respective roles. Auditdata also informs its personnel of possible consequences of breaching the security rules and procedures.

Auditdata will only use anonymous data in training.

Auditdata Personnel will not process Customer Data without authorization from Customer. Auditdata personnel are obligated to maintain the security and secrecy of any Customer Data and this obligation continues even after their engagements end.

Product Development, IT Operations and Support staff may have access to data (only where necessary on a need to know basis)

18.1.5 Domain: Physical and environmental security

Physical access to facilities. Auditdata (including subcontractors) limits access to facilities where information systems that process Personal Data are located to identified authorized individuals.

Physical access to components. Auditdata maintains records of the incoming and outgoing media containing Personal Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of Personal Data they contain.
Protection from disruptions. Auditdata uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.
Component disposal. Auditdata uses industry standard processes to delete Personal Data when it is no longer needed.

18.1.6 Domain: Communications and operations management

Operational policy. Auditdata maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Personal Data.

18.1.7 Data recovery procedures

The data centre operating the Auditdata products and services include replication features that facilitate recovery of Personal Data in the event a particular machine or cluster within an Auditdata

+45 70 20 31 24
www.auditdata.com
info@auditdata.com

data centre fails. The Auditdata products and services include a regular data backup procedure in addition to the data centre replication. Auditdata is obligated to take backup of data stored within the Software according to Auditdata's backup and data recovery procedure which is described below. If Customer wants additional safety measures, then Customer is responsible for taking additional steps to provide added fault tolerance, such as creating historical backups of Personal Data, storing backups of Personal Data off the platform, etc.

Auditdata cloud backup and data recovery procedure – SOP 30.0243, Auditdata internal IT backup and restore procedure in accordance with SOP 30.0251:

On an ongoing basis, but in no case less frequently than once a week (unless no Personal Data has been updated during that period), Auditdata maintains multiple copies of Personal Data from which Personal Data can be recovered.

Auditdata stores encrypted copies of Personal Data and data recovery procedures in a different place from where the primary computer equipment processing the Personal Data is located.

Auditdata has specific procedures in place governing access to copies of Personal Data.

Auditdata logs data restoration efforts, including the description of the restored data, and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.

Personal Data not covered by Auditdata Operations SLA's (e.g. temporary databases or data files for migration or trouble shooting etc.) is specifically chosen to not be covered by backup procedures, to reduce risk of non-compliance to data retention requirements.

18.1.8 Malicious software

Auditdata has anti-malware controls to help avoid malicious software gaining unauthorized access to Personal Data, including malicious software originating from public networks.

18.1.9 Data beyond boundaries

Auditdata provides encrypting Personal Data transmitted to and from its data centres over public networks. Auditdata uses encryption for replication of non-public Personal Data between its data centres.

Auditdata restricts access to Personal Data in media leaving its facilities (e.g., through encryption). Event logging. Auditdata logs, or enables the data exporter to log, access and use of information systems containing Personal Data, registering the access ID, time, authorization granted or denied, and relevant activity.

18.2 Domain: Access control

Access policy. Auditdata maintains a record of security privileges of individuals having access to Personal Data.

18.2.1 Access authorization

+45 70 20 31 24
www.auditdata.com
info@auditdata.com

Auditdata maintains and updates a record of personnel authorized to access its systems that contain Personal Data.

Auditdata deactivates authentication credentials that have not been used for a period of time not to exceed twelfth months.

Auditdata identifies those personnel who may grant, alter, or cancel authorized access to data and resources.

Auditdata ensures that where more than one individual has access to systems containing Personal Data, the individuals have separate identifiers/logins.

18.2.2 Least privilege

Technical support personnel are only permitted to have access to Personal Data when needed.

Auditdata restricts access to Personal Data to only those individuals who require such access to perform their job function.
Integrity and confidentiality. Auditdata instructs its personnel to disable administrative sessions when leaving premises its controls or when computers are otherwise left unattended.

18.2.3 Authentication

Auditdata uses industry standard practices to identify and authenticate users who attempt to access information systems.

Where authentication mechanisms are based on passwords, Auditdata requires that the passwords are renewed regularly.

Where authentication mechanisms are based on passwords, Auditdata requires the password to be at least eight characters long.

Auditdata ensures that deactivated or expired identifiers are not granted to other individuals.
Auditdata monitors or enables the data exporter to monitor repeated attempts to gain access to Personal Data using an invalid password.

Auditdata maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

Auditdata uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

Network design. Auditdata has controls to avoid individuals assuming access rights they have not been assigned to gain access to Personal Data they are not authorized to access.

18.3 Domain: Information security incident management

Incident response process. Auditdata maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.

+45 70 20 31 24
www.auditdata.com
info@auditdata.com

Service Monitoring. Auditdata security personnel verify logs at least every six months to propose remediation efforts if necessary.

18.4 Domain: Business Continuity Management

Auditdata maintains emergency and contingency plans for the facilities in which its information systems that process Personal Data are located.

Auditdata's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Personal Data to its last replicated state from before the time it was lost, unless it has been specifically decided to not keep data under backup, for data retention requirements compliance.

18.5 Home/remote working

Working outside of Auditdata's premises is called "Teleworking". While working outside of Auditdata's premises, can users connect to the Auditdata network using our secure Jumphost/direct access VPN connections.

Auditdata cannot protect user's private computer against virus and theft, and users are not allowed to use this equipment to work with Auditdata information or transfer data between your private computer and the work computer.

Company Computers (desktop and laptops) are protected by being properly enrolled to the Auditdata domain involving corporate managed access control, software patching, secure DNS (domain name server), antivirus system and global policies for local firewall management and automatic timeout screen lock protection. In addition, all laptop computers must have hard disk encryption activated.

18.6 Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance – assist the data controller in accordance with Clause 9.1. and 9.2.

18.7 Storage period/erasure procedures

The Data Processor's processing of personal data on behalf of the Data Controller may be performed when this Data Processing Agreement commences. Processing has the following duration:

The Personal Data (PII/SPI) are stored during the Term of the Agreement and upon termination returned or deleted.

18.8 Processing location

- Processing of the personal data under this Data Processing Agreement cannot be performed at other locations than the following without the Data Controller's prior written consent:
- Microsoft Azure – EU data location (The purpose of engaging Microsoft is to utilize the Microsoft Azure hosting and storage facilities to provide the cloud-based services to Customer). Microsoft Azure is ISO 27001 certified.
- Auditdata headquarters. The headquarter is ISO 27001 the main certification site.
- Auditdata's sites (Daughters). Auditdata's sites processing data are ISO 27001 certified as sites under Auditdata A/S' s main certificate.

+45 70 20 31 24
www.auditdata.com
info@auditdata.com

- Auditdata's outsourced internal IT – EU data location (only where necessary on a need to know basis)

18.9 Instruction for or approval of the transfer of personal data to third countries

The Data Processor only process data on EU and data locations in compliance with local data sovereignty.

Procedures for the Data Controller's inspection of the processing being performed by the Data Processor

There is not agreed any Procedures for the Data Controller's inspection of the processing being performed by the Data Processor.

Procedures for inspection of the processing being performed by sub-processors
There is not agreed any Procedures for inspection of the processing being performed by sub-processors.