DATED

DATA PROCESSING AGREEMENT

between

[CUSTOMER]

and

NavVis UK Ltd

CONTENTS

1. Definitions and Interpretation 2
2. Personal data types and processing purposes 4
3. Provider's obligations 5
4. Provider's employees 6
5. Security 6
6. Personal data breach 6
7. Transfers of personal data 7
8. Subcontractors 8
9. Complaints, data subject requests and third-party rights 8
10. Term and termination 9
11. Data return and destruction 10
12. Records 10
13. Audit 11
14. Use for Business Purposes 11
15. Indemnification 12
16. Confidentiality of Provider's security measures 12
17. Notice 12

ANNEX

ANNEX A Personal Data processing purposes and details 14
ANNEX B Technical and Organizational Measures 15

This agreement is dated [DATE] or, where no date is inserted, takes effect on the Effective Date.

PARTIES

(1) [CUSTOMER] incorporated and registered in [England and Wales] with company number [NUMBER] whose registered office is at [REGISTERED OFFICE ADDRESS] or, where these details are not completed, the customer entity that is party to the Master Agreement with the Provider (**Customer**)

(2) NavVis UK Ltd incorporated and registered in England and Wales with company number 14279485 whose registered office is at Roedl Legal Limited, 170 Edmund Street, Birmingham, United Kingdom, B3 2HB (**Provider**)

BACKGROUND

(A) The Customer and the Provider have entered into [an [AGREEMENT] on [INSERT DATE]] or, where these details are not completed, one or more agreements under which the Provider provides NavVis products and/ or services to the Customer (**Master Agreement**) that may require the Provider to process Personal Data on behalf of the Customer.

(B) This personal data processing Agreement (**PDPA**) sets out the additional terms, requirements and conditions on which the Provider will process any such Personal Data when providing services under the Master Agreement. This PDPA contains the mandatory clauses required by Article 28(3) of the UK GDPR for contracts between controllers and processors.

AGREED TERMS

1. Definitions and Interpretation

The following definitions and rules of interpretation apply in this PDPA.

1.1 Definitions:

Authorised Persons: the Customer's account administrators for the services under the Master Agreement and any other persons or categories of persons that the Customer authorises to give the Provider written personal data processing instructions as identified in ANNEX A or otherwise notified to the Provider in writing.

Business Day: Monday to Friday, excluding public holidays in England and Wales.

Business Hours: the period from 9am to 5pm (London time) on a Business Day.

Business Purposes: the services to be provided by the Provider to the Customer as described in the Master Agreement and any other purpose specifically identified in ANNEX A.

Commission: the Information Commission established under section 114A, DPA 2018, or any successor supervisory authority.

Controller: has the meaning given in section 6, DPA 2018.

Data Protection Legislation: all applicable data protection and privacy legislation in force from time to time in the UK, including, without limitation, the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) (**DPA 2018**); and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) in each case as amended from time to time; and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications).

Data Subject: the identified or identifiable living individual to whom the Personal Data relates.

EEA: the European Economic Area.

Effective Date: the date on which this PDPA is signed by both parties or, where it is not signed separately, the date on which the Master Agreement incorporating it takes effect.

Personal Data: means any information relating to an identified or identifiable living individual that is processed by the Provider on behalf of the Customer as a result of, or in connection with, the provision of the services under the Master Agreement.

Processing, **processes**, **processed**, **process**: any activity that involves the use of the Personal Data. It includes, but is not limited to, any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring the Personal Data to third-parties.

Personal Data Breach: a breach of security leading to the accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, or access to, the Personal Data.

Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

Records: has the meaning given in Clause 12.1.

Term: this PDPA's term as defined in Clause 10.1(b).

UK GDPR: has the meaning given in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

1.2 This PDPA forms part of and is incorporated into the Master Agreement. Where this PDPA is referenced in or linked from a quote, order form or other document forming part of the Master Agreement, it binds the parties from the Effective Date without the need for separate signature. Interpretations and defined terms set forth in the Master Agreement apply to the interpretation of this PDPA, save where defined in this PDPA.

1.3 The Annexes form part of this PDPA and will have effect as if set out in full in the body of this PDPA. Any reference to this PDPA includes the Annexes.

1.4 A reference to writing or written excludes fax but not email.

1.5 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this PDPA and any provision contained in the Annexes, the provision in the body of this PDPA will prevail;

(b) any of the provisions of this PDPA and the provisions of the Master Agreement relating to the processing of Personal Data, the provisions of this PDPA will prevail to the extent of that conflict, save that Clause 15.2 governs the limitation of liability.

2. Personal data types and processing purposes

2.1 The Customer and the Provider agree and acknowledge that for the purpose of the Data Protection Legislation:

(a) the Customer is the Controller, and the Provider is the Processor;

(b) the Customer retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Legislation, including but not limited to, providing any required notices and obtaining any required consents, and for the written processing instructions it gives to the Provider; and

(c) ANNEX A describes the subject matter, duration, nature and purpose of the processing and the Personal Data categories and Data Subject types in respect of which the Provider may process the Personal Data to fulfil the Business Purposes.

(d) Where the Customer processes the Personal Data as a processor on behalf of a third-party controller (e.g. Customer’s end customer), the Customer warrants that its instructions to the Provider have been authorised by that controller, the Provider acts as the Customer's sub-processor, and the Customer will be the Provider's sole point of contact in relation to that controller.

3. Provider's obligations

3.1 The Provider will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's documented instructions, which consist of the Master Agreement, this PDPA, the Customer's use and configuration of the NavVis products and services, and any other written instructions from Authorised Persons, unless required to do so by domestic law, in which case the Provider will inform the Customer of that legal requirement before processing unless that law prohibits this on important grounds of public interest. The Provider will not process the Personal Data for any other purpose or in a way that does not comply with this PDPA or the Data Protection Legislation. The Provider must immediately notify the Customer if, in its opinion, the Customer's instructions do not comply with the Data Protection Legislation and may suspend performance of the instruction in question until the Customer confirms or modifies it following that notification.

3.2 Insofar as reasonably and practicably possible the Provider must comply promptly with any Customer written instructions requiring the Provider to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

3.3 The Provider will maintain the confidentiality of the Personal Data and will not disclose the Personal Data to third parties unless the Customer or this PDPA specifically authorises the disclosure, or as required by domestic law, court or regulator (including the Commission). If a domestic law, court or regulator (including the Commission) requires the Provider to process or disclose the Personal Data to a third-party, the Provider must first inform the Customer of such legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the domestic law prohibits the giving of such notice.

3.4 The Provider will reasonably assist the Customer, at the Customer's request and, save where the assistance is required due to the Provider's breach of this PDPA, at the Customer's reasonable cost, with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of the Provider's processing and the information available to the Provider, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with the Commission under the Data Protection Legislation.

3.5 The Provider must notify the Customer promptly if it becomes aware that any change to the Data Protection Legislation is likely to adversely affect the Provider's ability to perform this PDPA.

4. Provider's employees

4.1 The Provider will ensure that all of its employees and other persons authorised to process the Personal Data:

(a) are informed of the confidential nature of the Personal Data and are bound by written confidentiality obligations and use restrictions in respect of the Personal Data;

(b) have undertaken training on the Data Protection Legislation and how it relates to their handling of the Personal Data and how it applies to their particular duties; and

(c) are aware both of the Provider's duties and their personal duties and obligations under the Data Protection Legislation and this PDPA.

5. Security

The Provider must at all times maintain appropriate technical and organisational measures against accidental, unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the technical and organizational measures set out in Annex B. The Provider may update the security measures in ANNEX B from time to time, provided that such updates do not materially reduce the overall level of protection of the Personal Data.

6. Personal data breach

6.1 The Provider will without undue delay notify the Customer in writing if it becomes aware of:

(a) the loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data. Where this results from the Provider’s breach of this PDPA, the Provider will use all reasonable endeavours to restore such Personal Data from its backups at its own expense as soon as possible;

(b) any accidental, unauthorised or unlawful processing of the Personal Data; or

(c) any Personal Data Breach.

6.2 Where the Provider becomes aware of any event under clause 6.1 (a), (b) and/or (c) above, it will, without undue delay, also provide the Customer with the following written information, to the extent reasonably available:

(a) a description of the nature of (a), (b) and/or (c), including the categories of in-scope Personal Data and approximate number of both Data Subjects and the Personal Data records concerned;

(b) the likely consequences; and

(c) a description of the measures taken or proposed to be taken to address (a), (b) and/or (c), including measures to mitigate its possible adverse effects.

6.3 Following any accidental, unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter to such an extent as is reasonably required. Further, the Provider will reasonably co-operate with the Customer in the Customer's handling of the matter, by:

(a) assisting with any investigation;

(b) providing the Customer with relevant information about any facilities and operations affected and, for facilities under the Provider's control, physical access on reasonable notice where reasonably necessary;

(c) facilitating interviews with the Provider's relevant employees and others under its control involved in the matter;

(d) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Customer; and

(e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorised or unlawful Personal Data processing.

6.4 The Provider will not inform any third-party of any accidental, unauthorised or unlawful processing of all or part of the Personal Data and/or a Personal Data Breach without first obtaining the Customer's written consent, except to its subcontractors, professional advisers and insurers on a confidential basis, or when required to do so by domestic law.

6.5 The Provider will cover all reasonable expenses associated with the performance of the obligations under clause 6.1 to clause 6.3 unless the matter arose from the Customer's specific written instructions, negligence, wilful default or breach of this PDPA or the Master Agreement, in which case the Customer will cover the Provider's reasonable expenses associated with the performance of those obligations.

7. Transfers of personal data

The Provider (and any subcontractor) must not transfer or otherwise process the Personal Data outside the UK or the EEA without obtaining the Customer's prior written consent.

8. Subcontractors

8.1 The Provider may only authorise a third-party (subcontractor) to process the Personal Data if:

(a) the Customer is provided with an opportunity to object, on reasonable data protection grounds, to the appointment of each new or replacement subcontractor within 10 Business Days after the Provider notifies the Customer in writing (including by email) of such subcontractor's name, location and processing activities. If the Customer objects and the parties do not resolve the objection in good faith within 30 days, either party may terminate the affected services under the Master Agreement on written notice;

(b) the Provider enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this PDPA, in particular, in relation to requiring appropriate technical and organisational data security measures; and

(c) the Provider maintains control over all of the Personal Data it entrusts to the subcontractor.

(d) The Provider must carefully select each subcontractor, having regard in particular to the suitability of the technical and organisational measures put in place by the subcontractor, and to the Provider's obligations under Clause 0 where the subcontractor processes the Personal Data outside the UK or the EEA.

8.2 Those subcontractors approved as at the commencement of this PDPA are as set out in ANNEX A. The Provider must keep Annex A updated to reflect any subcontractor approved in accordance with this Clause 8 and include any subcontractor's name and location and the contact information for the person responsible for privacy and data protection compliance.

8.3 Where the subcontractor fails to fulfil its obligations under the written agreement with the Provider which contains terms substantially the same as those set out in this PDPA, the Provider remains fully liable to the Customer for the subcontractor's performance of its agreement obligations.

8.4 Reserved.

9. Complaints, data subject requests and third-party rights

9.1 The Provider must, subject to Clause 9.4, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:

(a) the rights of Data Subjects under the Data Protection Legislation, including, but not limited to, subject access rights, the right to make a complaint, the rights to rectify, port and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

(b) information or assessment notices served on the Customer by the Commission under the Data Protection Legislation.

9.2 The Provider must notify the Customer without undue delay in writing if it receives any complaint, notice or communication that relates to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation in respect of the Personal Data.

9.3 The Provider must notify the Customer without undue delay, and in any event within 5 Business Days, if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation.

9.4 The Provider will give the Customer its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request. Where this relates to the Provider's breach of this PDPA, the Provider will bear its own costs of providing that co-operation and assistance; in all other cases, the Customer will reimburse the Provider's reasonable costs of providing that co-operation and assistance.

9.5 The Provider must not disclose the Personal Data to any Data Subject or to a third-party other than in accordance with the Customer's written instructions, or as required by domestic law.

10. Term and termination

10.1 This PDPA will remain in full force and effect so long as:

(a) the Master Agreement remains in effect; or

(b) the Provider or any subcontractor retains any of the Personal Data related to the Master Agreement in its possession or control (including any such data in back-up IT systems) (**Term**).

10.2 Any provision of this PDPA that expressly or by implication should come into or continue in force on or after termination of the Master Agreement in order to protect the Personal Data will remain in full force and effect.

10.3 A material breach by the Provider of the terms of this PDPA that is not remedied within 30 days of written notice from the Customer specifying the breach and requiring it to be remedied will be treated as a material breach of the Master Agreement. In such event, the Customer may terminate any part of the Master Agreement involving the

processing of the Personal Data on written notice to the Provider, without further liability or obligation of the Customer.

10.4 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Master Agreement obligations, the parties may agree to suspend the processing of the Personal Data until that processing complies with the new requirements.

11. Data return and destruction

11.1 The Customer may at any time during the Term retrieve all or part of the Personal Data itself using download and export functionality of the NavVis services, and such retrieval constitutes the return of the Personal Data for the purposes of this PDPA. Only where the Customer is unable to retrieve Personal Data using that functionality for reasons attributable to the Provider will the Provider, at the Customer's written request, provide reasonable assistance to make that Personal Data available to the Customer in a commonly used, machine-readable format.

11.2 Unless otherwise agreed in writing, the Customer may continue to retrieve the Personal Data in accordance with Clause 11.1 for 30 days after termination or expiry of the Master Agreement for any reason, and the Customer is responsible for retrieving any Personal Data it wishes to keep within that period. Subject to the provisions of clause 11.3, the Provider will securely delete or destroy all Personal Data related to this PDPA in its possession or control within three months of termination or expiry of the Master Agreement. This clause does not apply to the extent domestic law requires the Provider to retain the Personal Data, in which case the Provider will continue to protect it in accordance with this PDPA.

11.3 Personal Data retained solely within the Provider's or their subcontractors' automated backup systems shall be deleted or destroyed in accordance with the Provider's or subcontractors' standard backup retention and deletion cycle, and this PDPA will continue to apply to such Personal Data until it is deleted or destroyed.

12. Records

12.1 The Provider will keep detailed, accurate and up-to-date written records regarding any processing of the Personal Data, including but not limited to, the access, control and security of the Personal Data, the processing purposes, categories of processing, and a general description of the technical and organisational security measures referred to in Clause 0 (**Records**).

12.2 The Provider will ensure that the Records are sufficient to enable the Customer to verify the Provider's compliance with its obligations under this PDPA and the Data Protection Legislation and the Provider will provide the Customer with copies of the Records upon request.

12.3 The Provider will review the information listed in the Annexes to this PDPA at least once a year to confirm its current accuracy and update it when required to reflect current practices. The Customer will notify the Provider of any changes to the information it has provided for the Annexes.

13. Audit

13.1 The Provider will make available to the Customer all information necessary to demonstrate compliance with this PDPA and will permit the Customer and its third-party representatives (who must not be competitors of the Provider and must be bound by confidentiality obligations) to audit the Provider's compliance with its PDPA obligations, on at least 10 Business Days' notice, during Business Hours, no more than once in any 12-month period (save as set out in Clause 13.2 or where required by the Commission), during the Term. The Provider may first respond to an audit request by providing relevant certifications, third-party audit reports or a completed security questionnaire, and an audit will take place only where these are reasonably insufficient to demonstrate compliance. Subcontractors will be audited by the Provider making available their relevant certifications and audit reports. The Provider will give the Customer and its third-party representatives all necessary assistance to conduct such audits at no additional cost to the Customer. The assistance may include, but is not limited to:

(a) access to, and copies of, the Records and any other relevant information held at the Provider's premises or on systems storing the Personal Data;

(b) access to and meetings with any of the Provider's personnel reasonably necessary to provide all explanations and perform the audit effectively; and

(c) inspection of all Records and the infrastructure, electronic data or systems, facilities, equipment or application software under the Provider’s control used to process the Personal Data, in a manner that does not compromise the security or confidentiality of other customers’ data.

13.2 The notice requirements in Clause 13.1 will not apply if the Customer has reasonable grounds to believe that a Personal Data Breach has occurred or is occurring, or that the Provider is in material breach of any of its obligations under this PDPA or any of the Data Protection Legislation, in which case any audit under this Clause 13 will be limited to what is reasonably necessary to investigate that specific matter.

14. Use for Business Purposes

The Customer warrants and represents that the Provider's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Customer will comply with the Data Protection Legislation.

15. Indemnification

15.1 Each party agrees to indemnify the other party against all costs, claims, damages or expenses incurred by the other party or for which the other party has become liable due to any failure by the indemnifying party or its employees, subcontractors or agents to comply with any of its obligations under this PDPA and/or the Data Protection Legislation.

15.2 Notwithstanding Clause 15.11.5(b), each party's total aggregate liability 15arising out of or in connection with this PDPA (including under Clause 15.1) is subject to the limitations and exclusions of liability set out in the Master Agreement, save that nothing in this PDPA or the Master Agreement limits or excludes either party's liability for:

(a) death or personal injury caused by its negligence;

(b) fraud or fraudulent misrepresentation; or

(c) any matter that cannot be limited or excluded as a matter of law.

16. Confidentiality of Provider's security measures

The Customer will keep confidential all information relating to the Provider's technical and organisational security measures and any other business secrets of the Provider that the Customer learns specifically from or in connection with the processing of the Personal Data under this PDPA, and will not disclose any such information to a third party without the Provider's prior written consent, except to the extent such information is already in the public domain other than as a result of a breach of this Clause, or disclosure is required by domestic law, court or regulator (including the Commission). This Clause will survive termination or expiry of the Master Agreement.

17. Notice

17.1 Any notice given to a party under or in connection with this PDPA shall be in writing and shall be:

(a) delivered by hand or by pre-paid first-class post or other next working day delivery service at its registered office (if a company) or its principal place of business (in any other case); or

(b) sent by email to the following addresses (or an address substituted in writing by the party to be served):

(i) For the Customer: [CUSTOMER DATA PRIVACY CONTACT] or, if not completed, the email address of the Customer's contact designated in the Master Agreement or of its account administrator for the services

(ii) For the Provider: *privacy@navvis.com*, with copy to *martin.harrington@navvis.com*

17.2 Any notice shall be deemed to have been received:

(a) if delivered by hand, at the time the notice is left at the proper address; or

(b) if sent by pre-paid first-class post or other next working day delivery service, at 9:00am on the second Business Day after posting; or

(c) if sent by email (provided the sender has not received a delivery failure notification), at the time of transmission, or, if this time falls outside Business Hours in the place of receipt, when Business Hours resume.

17.3 This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

Where signed separately, this PDPA has been entered into on the date stated at the beginning of it; otherwise it takes effect on the Effective Date as part of the Master Agreement.

Signed by [NAME OF AUTHORISED SIGNATORY]	
for and on behalf of [NAME OF CUSTOMER]	Authorised signatory
Signed by [NAME OF AUTHORISED SIGNATORY]	
for and on behalf of NavVis UK Ltd	Authorised signatory

ANNEX A Personal Data processing purposes and details

Subject matter of processing: the processing of data uploaded by or on behalf of the Customer (including data captured by the Customer using NavVis hardware) using NavVis's post-processing software (NavVis IVION Processing) in the NavVis Cloud hosted on Amazon Web Services (AWS), and the provision/hosting of data using NavVis IVION in the NavVis Cloud hosted on Amazon Web Services (AWS), in each case in connection with the Master Agreement.

Duration of Processing: for the duration of the Master Agreement, in accordance with the duration of the services provided under it, and thereafter until the Personal Data is returned or deleted in accordance with Clause 11.

Nature of Processing: receipt of data uploaded by or on behalf of the Customer (including data captured with NavVis hardware); storage, post-processing and analysis of data via NavVis's post-processing software; and hosting and provision of processed data via NavVis IVION, in each case using NavVis Cloud infrastructure hosted on Amazon Web Services (AWS).

Business Purposes: providing the NavVis products and services described in the Master Agreement, including capturing, processing, storing and hosting data in connection with those products and services.

Personal Data Categories: name; contact details (address, email, telephone); job title; user account, access and log data of the Customer's authorised users (such as user name, email address, IP address and usage data); images of persons and vehicle number plates (in whole or in part); and any other personal data contained in the scans, images, point clouds, annotations or other content uploaded by or on behalf of the Customer.

Data Subject Types: The Customer's employees and other authorised users of the services; the Customer's suppliers and customers; and other individuals (including visitors and members of the public) captured in data uploaded by or on behalf of the Customer.

Authorised Persons: the Customer's account administrators for the services and any other persons notified by the Customer to the Provider in writing.

Approved Subcontractors:

- NavVis GmbH, Blutenburgstr. 18, D-80636 Munich, Germany, for the purpose of operating, post-processing, support and provision of NavVis IVION, IVION Go and NavVis IVION Processing.
- Amazon Web Services EMEA SARL (AWS), 38 avenue John F. Kennedy, L-1855 Luxembourg (http://aws.amazon.com), engaged by NavVis GmbH for the purpose of data hosting in AWS data centres located in the EU and/or the UK. AWS is certified to ISO 9001, ISO 27001, ISO 27017, ISO 27018, SOC 1/ISAE 3402, SOC 2, SOC 3, PCI DSS Level 1 and BSI C5.

ANNEX B Technical and Organizational Measures

The Provider has implemented the following technical and organisational data security measures:

1. Confidentiality

1.1 Entry control

Requirement:

The rooms in which personal data are processed or data processing systems are installed may not be freely accessible. They must be locked when employees are away. Entry authorizations must be assigned in a regulated procedure on a need-to-know basis and are generally monitored in terms of whether they are necessary. Rooms in which data processing systems (datacenter, server, network distributor, etc.) are located must have particular entry protections and may be accessible only to employees in IT administration (management, if necessary). Alternately, the devices must be stored in suitable and locked cabinets. Visitors and non-company individuals must be registered in a documented procedure and monitored while visiting the offices.

The company has implemented the requirement as follows:

☒ Locked building

☒ Locked offices

☒ Electronic security locking system

☒ Documented key assignment process

☒ Visitor accompaniment

☒ Loackable Floors

☒ Area-dependent authorization IDs

☒ Locked server rooms with entry control

☒ Locked server cabinets

☒ Alarm system for building / offices

☒ Elektronic entry control

☒ External guard on site

☒ Installed Security Cameras

1.2. Access control

Requirement:

For every network user, a personally assigned user must be set up with a minimum 10-digit password featuring both uppercase and lowercase letters, numbers, and special characters. The system must require users to change passwords at least every 90 days. Network users are to be required to comply with the user access policy in a manner subject to documentation. Creating, changing, and removing access authorizations must occur in a documented procedure. The establishment, modification and withdrawal of system access authorization must follow a documented procedure. Established system access authorizations must be regularly reviewed for their necessity and the review documented. Network access must be monitored and logged, including unsuccessful login attempts. Network access must be automatically blocked by the system after 10 failed attempts.

The company has implemented the requirement as follows:

☒ Personalized user

☒ Password convention with complex password having a minimum 8 of characters

☒ Central authentication with username and password

☒ Encrypted notebooks

☒ Secure link for external access

☒ Logging external access

☒ Use of an updated firewall

☒ Use of a mobile device management software

1.3 Usage control

Requirement:

A documented, role-based authorization concept must be provided for use of personal data which limits the use so that only authorized individuals can use the personal data necessary for their task (De Minimis Principal). The password rules for access control must also be followed for usage control. Administrative activities must be limited to a small group of

administrators. Administrator activities must be monitored and logged to the extent that the effort involved is technically supportable.

The company has implemented the requirement as follows:

☒ Role-based authorization concept

☒ User-dependent authentication with username and password

☒ Logging of user usage

☒ Encryption of mobile data media

☒ Assignment of authorizations only after approval by the data owner

☒ Safekeeping of the data media

☒ Compliant destruction of digital storage options

☒ Compliant destruction of paper documents

☒ Logged destruction

☒ Administrative users are kept to a minimum and documented.

1.4 Pseudonymization

Requirement:

Evaluations must be pseudonymized in so far as the connection to the individual is not absolutely necessary for the result.

The company has implemented the requirement as follows:

☒ Pseudonymization takes place immediately upon request of the Controller.

1.5 Separation control

Requirement:

Separation of personal data must be ensured through different storage locations or client separation.

The company has implemented the requirement as follows:

☒ Data storage on physically separate systems

☒ Client separation within the data processing system

☒ Separation of production and test systems

2. Integrity

2.1 Transfer control

Requirement:

Transfer control requires that only authorized individuals can inspect the personal data. For transmission by email, appropriate protective measures (e.g., encryption of communication between the email servers) are required. Mobile devices or mobile storage media must be encrypted if personal data are stored on them.

The company has implemented the requirements as follows:

☒ VPN connections

☒ Personal storage media use prohibited

☒ Special protection for the physical transport of data media

☒ Transfer of data in anonymized or pseudonymized form

☒ Self-hosted Text-Sharing Tool

2.2 Input control

Requirement:

It must be possible to assign the input, change, and deletion of personal data to the acting employee. The system must limit the change and deletion of datasets in order to effectively prevent accidental change or deletion.

The company has implemented the requirements as follows:

☒ Traceability of inputs, changes, and deletions by personalized users

☒ Traceability in assigning, changing, and deleting user authorizations

☒ Monitoring and logging automated data processing

2.3 Commissioned processing control

Requirement:

As part of commissioned processing control, commissioned data processing operations can only be carried out on the instructions of Controller. For this purpose, employees tasked with data processing must be trained and instructed on how to perform this task. Commissioned processing must be monitored through internal controls. The results of the controls must be documented.

Subcontractors may only be hired on the basis of the rules agreed upon with Controller. Transmission or access to personal data may not take place until the subcontractor has signed a commissioned processing agreement in accordance with Article 28 GDPR and has confirmed compliance with the data protection policy. Processor's obligation to audit its subcontractors results from the commissioned processing agreement established with Controller.

The company has implemented the requirement as follows:

☒ Documentation of processing activities

☒ Careful selection of the processor

☒ No use of processors that are not subject to obligations imposed in accordance with Article 28 GDPR

☒ Written agreement with the subcontractor regarding the minimum standards for data protection

☒ Reasonable monitoring of the processor

☒ Ensuring compliant destruction or return of data after completion of assignment

3. Availability and reliability

Requirement:

Personal data must be processed on data processing systems that are subject to regular and documented patch management. No systems may be linked on the network that are outside of the manufacturer's maintenance cycles (especially not any Windows XP, Windows Server 2003, etc.). Security-related patches must be installed within 72 hours after being announced. Continuous availability of personal data must be guaranteed by means of redundant storage media and backups according to the latest technical standards. Data centers and server rooms must be state of the art (temperature control, fire protection, water penetration, etc.). Servers must have uninterrupted power supply (UPS) ensuring controlled shutdown without any loss of data.

The company has implemented the requirement as follows:

☒ Regular documented patch management for servers

☒ Data storage on storage systems

☒ Physically separate redundant data storage

☒ Uninterrupted power supply

☒ Climate control for servers

☒ Early fire detection

4. Procedure for regular review, assessment, and evaluation

Requirement:

A procedure must be implemented for reviewing data protection in the company. It must include the obligation of employees to maintain data secrecy, training and education of employees, and regular auditing of data processing procedures. The processing procedure performed for the Controller must also be documented before data processing begins. A complete reporting and management process must be introduced for data breaches and the protection of data subjects' rights. It must also include notification of the Controller.

The company has implemented the requirement as follows:

☒ Appointment of a data protection officer

☒ Regular documented training of employees involved in data processing

☒ Documented procedure for introduction, change, and discontinuation of procedures

☒ Regular auditing of procedures

☒ Regular auditing of the processors

☒ Regular review of technical advancements in accordance with Article 32 GDPR

☒ Jour Fixe to check the current state of affairs