

**INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT
FOR THE PERIOD 1. OCTOBER 2024 TO 30. SEPTEMBER 2025
ON THE DESCRIPTION OF SAAS SOLUTIONS GAPPORTAL AND
WHISTLEBLOWER SCHEME AND THE ASSOCIATED TECHNICAL
AND ORGANIZATIONAL SECURITY MEASURES AND OTHER
CONTROLS, THEIR DESIGN AND OPERATIONAL EFFECTIVENESS
RELATING TO THE PROCESSING AND PROTECTION OF PER-
SONAL DATA IN ACCORDANCE WITH THE GENERAL DATA PRO-
TECTION REGULATION AND THE DANISH DATA PROTECTION
ACT**

GAPSOLUTIONS A/S

CONTENT

1. INDEPENDENT AUDITOR'S OPINION	2
2. GAPSOLUTIONS STATEMENT.....	5
3. GAPSOLUTIONS DESCRIPTION OF SAAS SOLUTIONS GAPPORAL AND WHISTLEBLOWER SCHEME	7
GAPSOLUTIONS A/S	7
SaaS Solutions GapPortal and Whistleblower scheme and Processing Of Personal Data	7
Management of the security of personal data.....	7
Risk Assessment	10
Technical and Organisational Security Measures and Other Controls	10
Changes from 1 October 2024 to 30 September 2025	14
Complementary Controls for Data Controllers	14
4. CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND TEST RESULTS.....	15
Control Area A	17
Control Area B	19
Control Area C	26
Control area D	29
Control Area E	30
Control Area F.....	31
Control Area H.....	34
Control Area I.....	35
Control area J	37

1. INDEPENDENT AUDITOR'S OPINION

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT FOR THE PERIOD 1 OCTOBER 2024 TO 30 SEPTEMBER 2025 ON THE DESCRIPTION OF THE SAAS SOLUTIONS GAPPORTAL AND WHISTLE-BLOWER SCHEME AND THE ASSOCIATED TECHNICAL AND ORGANISATIONAL SECURITY MEASURES AND OTHER CONTROLS, THEIR DESIGN AND OPERATIONAL EFFECTIVENESS RELATING TO THE PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE GENERAL DATA PROTECTION REGULATION AND THE DATA PROTECTION ACT

To: The Management of GapSolutions A/S
GapSolutions A/S' Customers (data controllers)

Scope

We have been tasked with providing a declaration of the description prepared by GapSolutions (the data processor) for the entire period 1 October 2024 to 30 September 2025 in section 3 of SaaS Solutions GapPortal and Whistleblower scheme and the associated technical and organizational security measures and other controls, aimed at the processing and protection of personal data in accordance with the Regulation of the European Parliament and of the Council on the protection of natural persons in connection with the processing of personal data and on the free movement of such data (the General Data Protection Regulation) and the Act on Supplementary Provisions to the General Data Protection Regulation (the Data Protection Act), and on the design and operational effectiveness of the technical and organizational security measures and other controls linked to the control objectives stated in the description.

Responsibilities of the Data Processor

The data processor is responsible for preparing the statement in section 2 and the accompanying description, including the completeness, accuracy, and manner in which the statement and description are presented. The data processor is also responsible for providing the services covered by the description; stating the control objectives; and designing and implementing controls to achieve the stated control objectives.

Auditor independence and quality management

We have complied with the requirements of independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Guidelines for Auditors' Ethical Conduct (IESBA Code), which is based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional conduct, as well as ethical requirements applicable in Denmark.

BDO Statsautoriseret Revisionspartnerselskab applies to the International Standard on Quality Management 1, ISQM 1, which requires us to design, implement and operate a quality management system, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable laws and other regulations.

Auditor's Responsibilities

Our responsibility is to express an opinion on the data processor's description and on the design and operating effectiveness of controls related to the control objectives stated in that Description, based on our procedures.

We have performed our work in accordance with ISAE 3000, Assurance Engagements Other than Audits or Reviews of Historical Financial Information. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether the description is fairly presented, in all material respects, and whether the controls are suitably designed and operating effectively.

An assurance engagement to provide a statement on the description, design, and operational effectiveness of controls at a data processor involves performing procedures to obtain evidence about the information in the data processor's description and about the design and operational effectiveness of the controls. The selected

procedures depend on the data processor's auditor's judgment, including the assessment of the risks that the description is not fairly presented and that the controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls, that we consider necessary to provide a high level of assurance that the control objectives stated in the description were achieved. A report assignment of this type also includes evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and the suitability of the criteria specified and described by the data processor in section 2.

It is our opinion that the evidence obtained is sufficient and appropriate to provide a basis for our conclusion.

Limitations of controls at a data processor

The data processor's description is prepared to meet the common needs of a broad range of data controllers and therefore may not include all the aspects of the use of SaaS Solutions GapPortal and Whistleblower scheme that each individual data controller may consider important based on their specific circumstances. Furthermore, due to their nature, controls at a data processor may not prevent or detect all breaches of personal data security. Additionally, any projection of the assessment of the operational effectiveness of controls to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Conclusion

Our conclusion is based on the matters outlined in this report. The criteria we used in forming our conclusion are the criteria described in the data processor's statement in section 2. It is our opinion that:

- a. that the description of SaaS Solutions GapPortal and Whistleblower scheme and the associated technical and organizational security measures and other controls aimed at the processing and protection of personal data in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act, as they were designed and implemented throughout the period 1 October 2024 to 30 September 2025, is fairly presented in all material respects, and
- b. that the technical and organizational security measures and other controls related to the control objectives stated in the description were suitably designed throughout the period 1 October 2024 to 30 September 2025, and
- c. that the tested technical and organizational security measures and other controls, which were necessary to provide a high level of assurance that the control objectives in the description were achieved in all material respects, operated effectively throughout the period 1 October 2024 to 30 September 2025.

Description of tests of controls

The specific controls tested, and the results of these tests are set out in section 4.

Intended users and purposes

This report is intended only for data controllers who have used the data processor's SaaS Solutions GapPortal and Whistleblower scheme and who have sufficient understanding to consider it along with other information, including the technical and organizational security measures and other controls that the data controllers themselves have implemented, when assessing whether the requirements of GDPR and the Danish Data Protection Act have been met.

Copenhagen, 3. November 2025

BDO Statsautoriseret Revisionspartnerselskab

Nicolai T. Visti
State Authorised Public Accountant

Mikkel Jon Larsen
Partner, head of Risk Assurance, CISA, CRISC

2. GAPSOLUTIONS STATEMENT

GapSolutions processes personal data in connection with SaaS Solutions GapPortal and Whistleblower scheme for our customers who are data controllers in accordance with the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation) and the Act on Supplementary Provisions to the General Data Protection Regulation (the Danish Data Protection Act).

The accompanying description is prepared for use of data controllers who have used SaaS Solutions GapPortal and Whistleblower scheme and who have sufficient understanding to consider the description along with other information, including the technical and organizational security measures and other controls that the data controllers themselves have implemented, when assessing whether the requirements of GDPR and the Danish Data Protection Act have been complied with.

GapSolutions A/S uses sub-processors. These sub-processors' relevant control objectives and related technical and organisational measures and other controls are not included in the accompanying description.

GapSolutions confirms that the accompanying description in section 3 provides fair description of SaaS Solutions GapPortal and Whistleblower scheme and the associated technical and organizational security measures and other controls throughout the period 1 October 2024 to 30 September 2025. The criteria used to give this opinion were that the accompanying description:

1. Describe SaaS Solutions GapPortal and Whistleblower scheme and how the associated technical and organizational security measures and other controls were designed and implemented, including an account of:
 - The types of services provided, including the type of personal data processed.
 - The processes in both IT systems and business procedures applied to process personal data and, if necessary, correct and delete personal data as well as limiting the processing of personal data.
 - The procedures used to ensure that data processing has taken place in accordance with contract, instructions, or agreement with the data controller.
 - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality.
 - The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation.
 - The procedures supporting in the event of breach of personal data security that the data controller may report this to the supervisory authority and inform the data subjects.
 - The procedures ensuring appropriate technical and organisational safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed.
 - The controls that we, with reference to the delimitation of SaaS Solutions GapPortal and Whistleblower scheme would have been designed and implemented by the data controllers, and which, if necessary to achieve the control objectives, are identified in the description.
 - The other aspects of the control environment, risk assessment process, information systems and communication, control activities and monitoring controls that are relevant to the processing of personal data.

2. Includes relevant information about changes in SaaS Solutions GapPortal and Whistleblower scheme and the associated technical and organizational security measures and other controls made during the period 1 October 2024 to 30 September 2025.
3. Does leave out or misrepresent information relevant to the scope of SaaS Solutions GapPortal and Whistleblower scheme and the associated technical and organizational security measures and other controls, considering that this description prepared to meet the common needs of a broad range of data controllers and therefore cannot include every aspect of SaaS Solutions GapPortal and Whistleblower scheme that each individual data controller may consider important according to their particular circumstances.

GapSolutions confirms that the technical and organizational security measures and other controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period 1 October 2024 to 30 September 2025. The criteria used to provide this statement were that:

1. The risks that threatened the achievement of the control objectives stated in the description were identified.
2. The identified controls, if performed as described, would provide a high level of assurance that the relevant risks would not prevent the achievement of the stated control objectives.
3. The controls were consistently applied as designed, including that manual controls were performed by people with appropriate competence and authority, throughout the period 1 October 2024 to 30 September 2025.

GapSolutions confirms that appropriate technical and organizational security measures and other controls have been implemented and maintained to meet agreements with the data Controllers, good data processing practices and relevant requirements for Data Processors in accordance with the GDPR and the Danish Data Protection Act.

Horsens, 3. November 2025

GapSolutions A/S

Jacob Barlach
Partner, IT & Marketing

3. GAPSOLUTIONS DESCRIPTION OF SAAS SOLUTIONS GAPPORAL AND WHISTLEBLOWER SCHEME

GAPSOLUTIONS A/S

GapSolutions A/S is a Danish-owned company that develops and operates a range of online systems (SaaS solutions) for public institutions as well as various industries in the private market.

GapSolutions A/S' approximately 40 employees are specialized in system development, server operation, support, and information security. They are organized into development, operations, support, finance, and administration.

The management and selected employees in the legal group oversee GapSolutions A/S' data protection in relation to the processing carried out on behalf of its customers. This includes entering data processing agreements, responding to inquiries from the data controller, reporting breaches of personal data security, compliance with internal policies and procedures, and similar activities.

SAAS SOLUTIONS GAPPORAL AND WHISTLEBLOWER SCHEME AND PROCESSING OF PERSONAL DATA

GapSolutions A/S provides the GapPortal and Whistleblower scheme as a Software-as-a-Service (SaaS) solution in accordance with customer contracts. The GapPortal and Whistleblower scheme are web-based cloud applications.

The GapPortal and Whistleblower scheme are developed in Denmark but hosted from a data center in Germany and Finland by the same sub-processor (Hetzner).

GapSolutions A/S processes personal data on behalf of its customers, who are data controllers, when they use GapPortal to upload and create documentation for compliance with different legislations. GapSolutions A/S also processes personal data on behalf of its customers, who are data controllers, when they use the Whistleblower scheme as part of establishing an internal Whistleblower scheme, which may arise from a legal obligation for the data controller under the Whistleblower Act § 9.

The personal data processed falls under Article 6 of the data protection regulation concerning general personal data and includes, among other things, personal names, email addresses, phone numbers, and identification. Additionally, special, and sensitive personal data may be processed in connection with reports received as part of the Whistleblower scheme. In this context, the data controller determines the purpose and legal basis for processing the information.

MANAGEMENT OF THE SECURITY OF PERSONAL DATA

GapSolutions A/S has established requirements for the establishment, implementation, maintenance, and continuous improvement of a management system for personal data security to ensure compliance with agreements with data controllers, good data processing practices, and relevant requirements for data processors in accordance with the data protection regulation and data protection act.

The technical and organizational security measures and other controls for the protection of personal data are designed based on risk assessments and implemented to ensure confidentiality, integrity, and availability, as well as compliance with applicable data protection legislation. Security measures and controls are automated and technically supported by IT systems wherever possible.

Relevant organizational and technical measures

The management of personal data security and the technical and organizational security measures and other controls are structured into the following main areas, for which control objectives and control activities are defined:

CONTROL AREA	SUB-CONTROL AREA	GDPR ARTICLE
A - Processing of personal data on behalf of the data controller's instructions	A.1 - Procedure for processing personal data	Article 28, sec. 3
	A.2 - Compliance with instructions for the processing of personal data	Article 28, sec. 3 and Articles 29 and 32 sec. 4
	A.3 - Notification of the data controller in the event of an illegal instruction	Article 28, sec. 3, letter h
	A.4 - Record of processing activities	Article 30, sec. 2, 3 and 4
B - Technical measures	B.1 - Agreed security measures	Article 28, sec. 3, letter c
	B.2 - Risk assessment	Article 28, sec. 3, letter c
	B.3 - Antivirus	Article 28, sec. 3, letter c
	B.4 - Firewall	Article 28, sec. 3, letter c
	B.5 - Network Security	Article 28, sec. 3, letter c
	B.6 – Access control - Access to personal data	Article 28, sec 3, letter c
	B.7 - Monitoring of systems and environments	Article 28, sec 3, letter c
	B.8 - Encryption during transmission of personal data	Article 28, sec. 3, letter c
	B.9 - Logging	Article 28, sec 3, letter c
	B.10 - Anonymization of personal data in development tasks	Article 28, sec. 3, letter c
	B.11 - Vulnerability scans and penetration tests	Article 28, sec. 3, letter c
	B.12 - Maintenance of system software	Article 28, sec. 3, letter c
	B.13 – Access control - Procedure and periodic review	Article 28, sec. 3, letter c
	B.14 - Logical access control	Article 28, sec. 3, letter c
	B.15 - Physical access control	Article 28, sec. 3, letter c
	B.16 - Backup and restoration	Article 28, sec. 3, letter c
	B.17 - Remote workplaces and remote access to systems and data	Article 28, sec. 3, letter c
C - Organizational measures	C.1 - Information security policies and information security policy review	Article 28, sec. 1
	C.2 - Information security policies in accordance with data processing agreements	Article 28, sec. 1
	C.3 – Employee recruitment - Screening	Article 28, sec. 1
	C.4 – Employee recruitment - Non-disclosure agreement and confidentiality agreement with employees and introduction to information security	Article 28, sec. 1 and Article 28. sec. 3, letter b
	C.5 – Employee termination - withdrawal of access rights and assets	Article 28, sec. 1
	C.6 – Employee termination - information on confidentiality and professional secrecy	Article 28, sec. 1 and Article 28, sec. 3, letter b
	C.7 – Awareness, education and training on Information security	Article 28, sec. 1
	C.8 - Supporter's access to personal data	Article 28, sec. 1
D - Deletion of personal data	D.1 - Deletion of data in compliance with the data controller's requirements	Article 28, sec. 3, letter g
	D.3 - Deletion and return of data upon termination of customer relationship	Article 28, sec. 3, letter g

CONTROL AREA	SUB-CONTROL AREA	GDPR ARTICLE
E - Retention of personal data	E.1 – Storage of data in compliance with the data controller	Article 28, sec. 3, letter c
	E.2 - Location of processing and storage of information	Article 28, sec. 3
F - Sub-processors	F.1 – Sub-processor agreement and instructions	Article 28, sec. 2 and 4
	F.2 - Approval of sub-processors	Article 28, sec. 2
	F.3 - Changes in approved sub-processors	Article 28, sec. 2
	F.4 - Obligations of the sub-processors	Article 28, sec. 2 and 4
	F.5 - Overview of sub-processors	Article 30, sec. 2
	F.6 - Supervision of sub-processors	Article 28, sec. 2 and 4
H - Data Subject Rights	H.1 - Procedure for fulfilling data subjects' rights	Article 28, sec. 3, letter e
	H.2 - Technical measures for fulfilling data subjects' rights	Article 28, sec. 3, letter e
I - Security Breaches	I.1 - Notification of personal data breaches	Article 33, sec. 2
	I.2 - Identification of Personal Data Breaches	Article 33, sec. 2
	I.3 - Timely notification of personal data breaches	Article 33, sec. 2
	I.4 - Assistance to data controllers in the event of personal data breaches	Article 28, sec. 3, letter f
J - Data protection by design and default settings	J.1 - Change management and privacy-by-design	Article 25
	J.2 - Implementing change in the production environment	Article 25
	J.3 - Separation of the development, test and production environment	Article 25
	J.4 - Access to source code	Article 25

Excluded Control Areas

The following control areas are not relevant to the services provided in this statement:

CONTROL AREA	SUB-CONTROL AREA	RATIONALE FOR THE EXCLUSION OF SPECIFIC CONTROL AREAS
C - Organizational measures	C.9 - Repair, service, and destruction of IT-equipment	These control activities are carried out by sub-processors. The data processor has conducted oversight of all sub-processors.
	C.10 - Data Protection Officer	The data processor is not required to appoint a formal Data Protection Officer (DPO).
D - Deletion of personal data.	D.2 - Requirements for storage and deletion period of data are following the data controller's requirements	No agreement has been made regarding the ongoing deletion of personal data in connection with the assurance services, and therefore this item is not applicable.
G – Transfer of personal data to third countries or international organisations.	G.1 - Procedure for transfers of personal data to third countries	This section is not applicable to this assurance report, as GapSolution A/S does not transfer personal data to third countries. All data processing takes place within the EU, and no US cloud providers are used.
	G.2 - Instructions for the transfer of personal data to third countries	
	G.3 - Valid transfer basis	

RISK ASSESSMENT

Management is responsible for initiating all initiatives that counteract the landscape threat that GapSolutions A/S faces at any given time, ensuring that established security measures and controls are appropriate, and that the risk of breaches to personal data security is reduced to an acceptable level.

An ongoing and at least annual assessment is conducted to determine the appropriate level of security. This assessment considers risks related to accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data transmitted, stored, or otherwise processed.

As a basis for updating technical and organizational security measures and other controls, an annual risk assessment is conducted. This risk assessment evaluates the likelihood and consequences of incidents that could threaten personal data security and the rights and freedoms of individuals, including accidental, intentional, and unintentional incidents. The risk assessment considers the current technical level and implementation costs.

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES AND OTHER CONTROLS

The technical and organisational security measures and other controls concern all processes and systems which process personal data on behalf of the Controller. The control objectives and control activities stated in the control schedule are an integral part of the subsequent description.

Processing of personal data on behalf of the data controller's instructions (control objective A)

Data processing agreement

GapSolutions A/S has implemented policies and procedures for entering into data processing agreements to ensure that GapSolutions A/S, in connection with the customer, enters into a data processing agreement that specifies the conditions for processing personal data on behalf of the data controller. GapSolutions A/S uses templates for data processing agreements in accordance with the services provided, including information

Instruction for processing of personal data

GapSolutions A/S has implemented policies and procedures to ensure that GapSolutions A/S acts in accordance with the instructions provided by the data controller in the data processing agreement. The instruction is maintained through procedures that instruct employees on how the processing of personal data should occur, including who can provide binding instructions to GapSolutions A/S at the data controller. The procedure also ensures that GapSolutions A/S informs the data controller when their instructions conflict with data protection legislation.

Register of Categories of Processing Activities

GapSolutions A/S has implemented policies and procedures to ensure that a register of categories of processing activities conducted on behalf of the data controller is maintained. The register is regularly updated and checked during the annual review of policies and procedures, etc. The register is kept electronically and can be made available to the supervisory authority upon request.

Technical measures (control objective B)

Agreed security measures

GapSolution A/S has implemented procedures to ensure that agreed security measures for the processing of personal data are established in accordance with the agreement with the data controller.

Risk Assessment

GapSolutions A/S has implemented technical and organizational security measures based on a risk assessment related to confidentiality, integrity, and availability.

Antivirus Program

GapSolutions A/S has implemented procedures to ensure that devices with access to networks and applications are protected against viruses and malware. Antivirus programs and other protection systems are continuously updated and adapted in response to the current threat level.

Firewall

GapSolutions A/S has implemented procedures to ensure that traffic between the internet and the network is controlled by a firewall. External access through firewall ports is minimized, and access rights are granted via specific ports to specific segments. Workstations use firewalls and anti-malware applications.

Network Security

GapSolutions A/S has implemented procedures to ensure that networks are divided into several virtual networks (VLANs), where traffic between the virtual networks is controlled by a firewall. Servers with built-in firewalls use them to ensure that only necessary services are accessed.

Logical access security and access management

GapSolutions A/S has implemented procedures to ensure that access to systems and data is protected by an authorization system. Users are created with a unique user ID and password, and user identification is used when granting access to resources and systems. All permissions assignment in systems is based on a work-related need. An evaluation of user's continued work-related need for access is conducted at least once a year, including a review of the relevance and accuracy of assigned user permissions. Procedures and controls support the process of creating, changing, and terminating users and granting rights, as well as reviewing them.

Multi-factor authentication is used when operating with critical systems. In cases where devices are stolen or otherwise compromised, the IT manager is immediately notified to close access.

Monitoring

GapSolutions A/S has implemented procedures to ensure ongoing monitoring of systems and implemented technical security measures.

External Communication Connections

GapSolutions A/S has implemented procedures to ensure that external communication connections are secured with strong encryption and that email and other communication containing sensitive personal data are encrypted during transmission using forced TLS.

Encryption of personal data

GapSolutions A/S has implemented procedures to ensure that databases containing personal data are encrypted, and the same applies to backups. Recovery keys and certificates are stored securely.

GapSolutions A/S has implemented procedures to ensure that data on personal devices which are not protected by special security measures are encrypted upon activation, so that access to the data is only possible for authorized users. Recovery keys and certificates are stored securely.

The algorithms and encryption levels used for encrypting devices, servers, and data are continuously assessed in relation to the current threat level.

Logging in Systems, Databases, and Networks

GapSolutions A/S has implemented procedures to ensure that logging is configured in accordance with legal requirements and business needs, based on a risk assessment of systems and the current threat level. The scope and quality of log data are sufficient to identify and detect any misuse of systems or data, and log data is regularly reviewed for usability and abnormal behavior. Log data is secured against loss and deletion.

Vulnerability scanning and penetration testing

GapSolution has implemented procedures to ensure that systems are in place to identify and address technical vulnerabilities in applications, services and infrastructure, thereby preventing the loss of confidentiality, integrity and availability of systems and data.

Maintenance of System Software

GapSolutions A/S has implemented procedures to ensure that system software is updated regularly according to the vendors' specifications and recommendations. Patch management procedures cover operating systems, critical services, and software installed on servers and workstations.

Physical Security

GapSolutions A/S has implemented procedures to ensure that premises are protected against unauthorized access. Only individuals with a work-related or other legitimate need have access to the premises, and special security measures have been introduced for areas where personal data is processed. Customers, suppliers, and other visitors are accompanied when visiting GapSolutions A/S offices.

Data Backup and Data Restoration

Data backups are outsourced to GapSolutions A/S' sub-processor Hetzner GMBH. Backup copies are stored in Germany and Finland by the same sub-processor. GapSolutions A/S has implemented procedures to ensure that residual tests are conducted annually.

Remote Workstations and Remote Access to Systems and Data

As GapSolutions A/S' employees often work "off-site", the devices used are configured to focus on device-centered security rather than using VPN. The hard drives of the employees' devices are encrypted as an example.

Organizational measures (control objective C)

Data Processor's Guaranteed

GapSolutions A/S has implemented policies and procedures to ensure that GapSolutions A/S can provide adequate assurances to implement appropriate technical and organizational security measures. GapSolutions A/S provides an annual update to customers in accordance with the data processing agreement. The description must include the technical and organizational security measures that are in place to protect personal data. GapSolutions A/S must also regularly demonstrate compliance with the agreed security measures, including in connection with audits and inspections conducted by the data controller.

Confidentiality and statutory confidentiality

GapSolutions A/S has implemented policies and procedures to ensure confidentiality in the processing of personal data. All employees at GapSolutions A/S have committed to confidentiality by signing an employment contract that includes terms of silence and confidentiality.

Supporter's access to personal data

GapSolutions A/S has implemented procedures for supporters' access to personal data, ensuring that supporters' access and handling of personal data during support tasks are based on support tickets and the supporters' work-related needs.

Erasure of personal data (control objective D)

Erasure of Personal Data

GapSolutions A/S has implemented policies and procedures to ensure that personal data is deleted in accordance with the data controller's instructions when the processing of personal data ceases upon the expiration of the contract with the data controller.

Storage of personal data (control objective E)

Storage of personal data

GapSolution A/S has implemented procedures to ensure that the storage of personal data is carried out solely in accordance with the contract with the data controller and the list of locations in the associated data processing agreement.

Retention of Personal Data

GapSolutions A/S has implemented procedures to ensure that the retention of personal data is only conducted in accordance with the contract with the data controller and the list of locations in the associated data processing agreement.

Sub-processors (control objective F)

GapSolutions A/S has implemented policies and procedures to ensure that sub-processors have been assigned the same data protection obligations as stated in the data processing agreement between the data controller and GapSolutions A/S, and that sub-processors can provide sufficient guarantees for the protection of personal data. Procedures ensure that the data controller gives prior specific or general written approval of sub-processors, including the management of changes to approved sub-processors.

GapSolutions A/S assesses the sub-processor and their guarantees before entering into an agreement to ensure that the sub-processor can comply with the obligations imposed on GapSolutions A/S. GapSolutions A/S conducts annual oversight of its sub-processors, based on a risk assessment of the specific processing of personal data, including obtaining auditor statements of the ISAE 3000, SOC 2, ISO 27001 certification, or similar documentation.

The data controllers utilising the SaaS solutions GapPortal and the Whistleblower scheme have not requested GapSolution A/S to provide notifications regarding audits conducted on sub-processors. Consequently, this control element is not included in the assurance report.

GapSolutions A/S exclusively uses sub-processors that are registered in EU and store data within the EU. Therefore, the assessment of insecure third-country transfers is not relevant for this statement.

GapSolutions A/S has established an overview of sub-processors, indicating the sub-processor's name, address, and description of the processing. Below is an overview of the sub-processors used for the services:

Sub-processor	Address	Location for data processing	Description of processing
Hetzner Online GmbH Datacenter Park Fallenstein DE 812871812	Industristr. 25 91710 Gunzenhausen Germany	Industristr. 25 91710 Gunzenhausen Germany	Hosting of servers
		Huurekuja 10 O4360 Finland	Hosting of backup
Flowmailer NL854692538B01	Van Nelleweg 1 3044 BC Rotterdam Nederland	Van Nelleweg 1 3044 BC Rotterdam Nederland	Mail Service

Data subjects' rights (control objective H)

Assistance to the Data Controller Regarding Data Subject Rights

GapSolutions A/S has implemented policies and procedures to ensure that GapSolutions A/S can assist the data controller in fulfilling their obligation to respond to requests to exercise the data subjects' rights.

Assistance to the Data Controller Regarding Processing Security and Impact Assessment

GapSolutions A/S has implemented policies and procedures to ensure that GapSolutions A/S can assist the data controller in ensuring compliance with the obligations in Article 32 regarding processing security and Article 35 regarding impact assessments.

Security breaches (control objective I)

Notification of Personal Data Breaches

GapSolutions A/S has implemented policies and procedures to ensure that personal data breaches are recorded with detailed information about the incident and that the data controller is notified without undue delay once GapSolutions A/S becomes aware of a breach of personal data security. The information provided enables the data controller to assess whether the breach of personal data security should be reported to the supervisory authority and whether the data subjects should be notified.

Assistance to the Data Controller Regarding Personal Data Breach

GapSolutions A/S has implemented policies and procedures to ensure that GapSolutions A/S can assist the data controller with notification and communication of personal data breaches regarding Article 33.

Data protection by design and default settings (control objective J)

Data Protection by Design and Default

GapSolutions A/S has implemented policies and procedures for the development and maintenance of the GapPortal and Whistleblower scheme, ensuring a controlled change process. A Change Management system is used to manage development and change tasks, and each task follows a consistent process that begins with a risk assessment in accordance with data protection by design and default requirements. Procedures for version control, logging, and backup are in place to facilitate reinstallation of previous versions.

Development, test, and production environments are separated, and there is a functional separation between employees in the development department and the operations and support department. Each development and change task undergo a testing phase, and anonymized production data is used as test data. Procedures for version control, logging, and backup have been implemented to enable the reinstallation of previous versions.

CHANGES FROM 1 OCTOBER 2024 TO 30 SEPTEMBER 2025

GapSolutions A/S has not made significant changes to the SaaS Solutions GapPortal and Whistleblower scheme and their associated technical and organisational security measures and other controls from 1 October 2024 to 30 September 2025.

COMPLEMENTARY CONTROLS FOR DATA CONTROLLERS

The data controller is responsible for implementing the following technical and organizational security measures and other controls to achieve the control objectives and thereby comply with data protection legislation:

- The data controller is responsible for ensuring that administrators' use of the GapPortal and Whistleblower scheme, and the processing of personal data within the system, complies with data protection legislation.
- The data controller manages user rights in the GapPortal and Whistleblower scheme, including which individuals are granted administrator access and what rights individual administrators are assigned.
- The data controller may not use the GapPortal and Whistleblower scheme for the processing, including storage, of sensitive personal data, and it is the data controller's responsibility to ensure that such personal data is not entered or uploaded into the GapPortal and Whistleblower scheme.

4. CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND TEST RESULTS

Purpose and scope

We conducted our engagement in accordance with ISAE 3000, Assurance Reports Other Than Audits or Reviews of Historical Financial Information.

BDO has undertaken actions to obtain evidence for the information in GapSolutions's description of SaaS Solutions GapPortal and Whistleblower scheme as well as for the design of the associated technical and organizational security measures and other controls. The procedures selected depend on BDO's judgement, including the assessment of the risks that the description is not fairly presented and that the controls are not suitably designed or operating effectively.

BDO's testing of the design and operational effectiveness of technical and organizational security measures and other controls has included the control objectives and associated control activities selected by GapSolutions, as detailed in the subsequent control sheet.

In the control sheet, BDO has described the tests performed, which were assessed necessary to provide a high level of assurance that the stated control objectives were achieved and that the associated controls were suitably designed and operated effectively throughout the period 1 October 2024 to 30 September 2025.

Performed test actions

Testing of the design of technical and organizational security measures and other controls, as well as their implementation and operational effectiveness, has been conducted by means of inquiry, inspection, observation and re-execution.

Type	Description
Inquiry	Inquiries of relevant personnel have been performed for all significant control activities. The purpose of the inquiries was to obtain knowledge and further information about implemented policies and procedures, including how the control activities are performed, and to obtain confirmed evidence of policies, procedures and controls.
Inspection	Documents and reports, which include information about the performance of the control, have been read for the purpose of assessing the design and monitoring of the specific controls, i.e., whether the design of the controls is such that they are expected to be effective if implemented, and whether the controls are sufficiently monitored and checked at suitable intervals. Tests have been performed of significant system structures of technical platforms, databases and network equipment to ensure that controls have been implemented, including for example assessment of logging, back-up, patch management, authorisations and access controls, data transmission, and inspection of equipment and locations.
Observation	The use and existence of specific controls have been observed, including tests to ensure that the control has been implemented.
Re-performance	Controls have been re-performed to obtain additional evidence that the controls operate as assumed.

For the services provided by Hetzner GMBH within hosting, we have received the received safety report and valid ISO 27001 certification for the sub data providers' technical and organisational security measures and other controls for the period 27 September 2022 to 26 September 2025.

For the services provided by Flowmailer B.V within the mail service, we have received valid ISO 27001 certification for the sub data providers' technical and organisational security measures and other controls for the period 28 January 2025 to 27 January 2028.

These relevant control objectives and associated controls of the sub-processor are not included in GapSolutions's description of SaaS Solutions GapPortal and Whistleblower scheme and the associated technical and organizational security measures and other controls. Therefore, we have only inspected the received documentation and tested the controls at GapSolutions that ensure proper supervision of the sub-processor's compliance with the data processing agreement between the sub-processor and the data processor, as well as compliance with the GDPR and the Danish Data Protection Act.

Test result

The result of the test made of technical and organizational measures and other controls has resulted in the following deviations noted.

A deviation exists when:

- Technical and organizational measures and other controls have not been designed or implemented to fulfil a control objective, and
- Technical and organizational measures and other controls related to a control objective are not suitably designed and implemented or did not operate effectively throughout the period.

Control Area A			
Control objectives			
Procedures and controls are complied to ensure that instructions regarding the processing of personal data are complied with in accordance with the entered into data processing agreement.			
No.	Control activity	Tests conducted by BDO	Test result
A.1	<p>Procedure for processing personal data</p> <ul style="list-style-type: none"> ▶ There are written procedures that stipulate that personal data processing may only be carried out when there is an instruction. ▶ An ongoing assessment is conducted – at least once a year – to determine whether the procedures need to be updated. 	<p>We have conducted inquiries with appropriate personnel at the data processor.</p> <p>We have inspected the data processor's privacy policy and observed that a formalized procedure is in place to ensure that personal data is processed strictly in accordance with instructions.</p> <p>We have inspected that the procedure includes a requirement for at least an annual assessment of the need for updates, including changes in the data controller's instructions or changes in data processing.</p> <p>We have inspected that in the reporting period the procedure is updated and approved by management.</p>	No exceptions noted.
A.2	<p>Compliance with instructions for processing personal data</p> <ul style="list-style-type: none"> ▶ The data processor only performs the processing of personal data that is stated in the instructions from the data controller. 	<p>We have conducted inquiries with appropriate personnel at the data processor.</p> <p>We have inspected the data processor's privacy policy and the most recent data processing agreement with a data controller and observed that the agreement contains instructions from the data controller.</p> <p>We have inspected the data processor's record of processing activities and by random inspection inspected that the processing is carried out in accordance with instructions from the data controller in the reporting period.</p>	No exceptions noted.

Control Area A			
Control objectives			
Procedures and controls are complied to ensure that instructions regarding the processing of personal data are complied with in accordance with the entered into data processing agreement.			
No.	Control activity	Tests conducted by BDO	Test result
A.3	<p>Notification of the data controller in the event of an illegal instruction</p> <p>▶ The data processor immediately notifies the data controller if an instruction, in the data processor's opinion, is in conflict with the GDPR or other EU or member state national data protection regulations.</p>	<p>We have conducted inquiries with appropriate personnel at the data processor.</p> <p>We have inspected the data processor's template for entering into data processing agreements with data controllers and the most recent data processing agreement with a data controller and observed that the data processor is obligated to notify the data controller in cases where an instruction is deemed to conflict with the law.</p> <p>Upon inquiry, we have been informed that there have been no cases where instructions have been assessed in violation of legislation during the reporting period.</p>	<p>We have been informed that there have been no incidents registered on illegal instructions within the reporting period. We have therefore not been able to test the control for implementation and effectiveness .</p> <p>No exceptions noted.</p>
A.4	<p>Record of processing activities</p> <p>▶ The Data Processor has established a list of categories of processing activities as a Data Processor. The list must include:</p> <ul style="list-style-type: none"> • the name and contact details of the data controller; • the categories of processing carried out on behalf of the controllers; • the name and contact details of each sub-processor; • indication of any transfer of personal data to a third country. <p>▶ The record shall be kept electronically and shall be made available to the supervisory authority upon request.</p>	<p>We have conducted inquiries with appropriate personnel at the data processor.</p> <p>We have inspected that the data processor's record of categories of processing activities as a data processor and observed that it contains relevant information, and that the record is stored electronically.</p> <p>We have inspected that the listing has been updated and/or approved.</p> <p>Upon inquiry, we have been informed that the Danish Data Protection Agency has not requested disclosure of the list during the reporting period.</p>	<p>We have been informed that the Danish Data Protection Agency did not request disclosure of the list at the time of the declaration. We have therefore not been able to test the control for implementation and effectiveness.</p> <p>No exceptions noted.</p>

Control Area B			
Control objectives			
Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant processing security.			
No.	Control activity	Tests conducted by BDO	Test result
B.1	<p>Agreed security measures</p> <ul style="list-style-type: none"> ▶ There are written procedures that require that agreed safeguards are put in place for the processing of personal data in accordance with the agreement with the data controller. ▶ An ongoing assessment is conducted – and at least once a year – to determine whether the procedures need to be updated. 	<p>We have conducted inquiries with appropriate personnel at the data processor.</p> <p>We have inspected that there are formalized procedures to ensure that the agreed security measures are established.</p> <p>We have inspected that the procedures are updated and approved during the reporting period.</p>	No exceptions noted.
B.2	<p>Risk assessment</p> <ul style="list-style-type: none"> ▶ The data processor has conducted a risk assessment and based on this implemented the technical measures deemed relevant to achieve appropriate security, including the agreed security measures with the data controller. 	<p>We have conducted inquiries with appropriate personnel at the data processor.</p> <p>We have conducted inquiries with appropriate personnel at the data processor. We have inspected that the data processor has conducted a risk assessment based on potential risks to the availability, confidentiality, and integrity of data concerning the rights of the data subject.</p> <p>We have inspected that the conducted risk assessment is updated and approved.</p> <p>We have randomly inspected that the data processor has implemented technical measures based on risk assessment, including measures agreed with the data controller.</p>	No exceptions noted.
B.3	<p>Antivirus</p> <ul style="list-style-type: none"> ▶ Antivirus is installed for the workstations and systems used for the processing of personal data, which is continuously updated. 	<p>We have conducted inquiries with appropriate personnel at the data processor.</p> <p>We have inspected one randomly selected workstation used for processing personal data to ensure that antivirus software is installed and updated.</p>	No exceptions noted.

Control Area B			
Control objectives			
Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant processing security.			
No.	Control activity	Tests conducted by BDO	Test result
		We have inspected data processing agreement between the data processor and the hosting provider and observed that an agreement has been made for the operation of servers, including protection against viruses.	
B.4	Firewall <ul style="list-style-type: none"> ▶ External access to systems and databases used for the processing of personal data is done through a secured firewall. 	<p>We have conducted inquiries with appropriate personnel at the data processor.</p> <p>We have inspected that external access to systems and databases used for the processing of personal data is only through the firewall.</p> <p>We have inspected that the firewall is configured according to internal policy for this.</p>	No exceptions noted.
B.5	Network security <ul style="list-style-type: none"> ▶ Internal networks are segmented to ensure limited access to systems and databases used for the processing of personal data. 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected the data processor's network topology and observed that networks are segmented to ensure limited access to systems and databases used for the processing of personal data.</p> <p>We have inspected documentation that the data processor's network is set up in accordance with the network topology.</p>	No exceptions noted.
B.6	Conditional access - access to personal data <ul style="list-style-type: none"> ▶ Access to personal data is isolated to users with a work-related need for it. 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that formalized procedures are in place to restrict users' access to personal information.</p>	No exceptions noted.

Control Area B			
Control objectives			
Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant processing security.			
No.	Control activity	Tests conducted by BDO	Test result
		<p>We have inspected that formalized procedures are in place to ensure that users' access to personal data is in accordance with their work-related needs.</p> <p>We have inspected that the agreed technical measures support the maintenance of the restriction on users' work-related access to personal data.</p> <p>We have inspected by means of a random sample of users' access to systems and databases that they are limited to the employees' work-related needs.</p>	
B.7	<p>Monitoring of systems and environments</p> <p>▶ For the systems and databases used for the processing of personal data, system monitoring with alarms has been established. The monitoring includes:</p>	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that systems and databases used for the processing of personal data have established system monitoring with alarms.</p>	No exceptions noted.
B.8	<p>Encryption for the transmission of personal data</p> <p>▶ Effective encryption is used when transmitting confidential and sensitive personal data via the internet and by e-mail.</p>	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected the use of encryption for transmissions of sensitive and confidential personal data via the internet or by e-mail.</p>	No exceptions noted.
B.9	<p>Logging</p> <p>▶ Logging has been established in systems, databases and networks for the following conditions:</p> <ul style="list-style-type: none"> • Activities performed by users • Activities of System Administrators and Others with Special Rights • Security incidents include: 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that logging of user activities in systems, databases and networks used for the processing and transmission of personal data is configured and enabled.</p>	No exceptions noted.

Control Area B			
Control objectives			
Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant processing security.			
No.	Control activity	Tests conducted by BDO	Test result
	<ul style="list-style-type: none"> ○ Changes to log setups, including disabling logging ○ Changes to system privileges for users ○ Failed log-in attempts to systems, databases and networks <p>▶ Log information is reviewed on an ongoing basis.</p>	<p>We have on sample basis inspected that logs have the expected content in relation to setup.</p> <p>We have inspected that logs are reviewed on an ongoing basis.</p>	
B.10	<p>Anonymisation of personal data in development tasks</p> <p>▶ Personal data used for development, testing or the like is always pseudonymized or anonymized form. The use is solely to fulfill the purposes of the data controller in accordance with the agreement and on their behalf.</p>	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>Upon inquiry, we have been informed that personal data is not present in the development environment; therefore, pseudonymisation or anonymisation of data is not applicable</p>	No exceptions noted.
B.11	<p>Vulnerability scans</p> <p>▶ The established technical measures are continuously tested by vulnerability scans.</p>	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that formalized procedures are in place for ongoing testing of technical measures, including the conduct of vulnerability scans.</p> <p>We have inspected by random samples that there is documentation of ongoing tests of the established technical measures.</p> <p>We have inspected that any deviations and weaknesses in the technical measures have been dealt with or accepted in a timely manner and satisfactorily.</p>	No exceptions noted.
B.12	<p>System Software Maintenance</p>	<p>We have conducted inquiries with appropriate personnel of the data processor.</p>	No exceptions noted.

Control Area B			
Control objectives			
Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant processing security.			
No.	Control activity	Tests conducted by BDO	Test result
	<ul style="list-style-type: none"> Changes to systems, workstations, databases, and networks follow established procedures that ensure maintenance with relevant updates and patches, including security patches. 	<p>We have inspected the configuration of update and patch settings on end user devices and observed an automated process. On a sample basis we have tested that the functionality works as intended.</p> <p>We have inspected data processing agreement between the data processor and Hetzner GMBH and observed that Hetzner GMBH is obligated to update and patch servers and databases.</p> <p>We have inspected the data processor's automated configuration for patch management on their infrastructure. On a sample basis we have tested that the functionality works as intended.</p>	
B.13	<p>Conditional Access - procedure and periodic review</p> <ul style="list-style-type: none"> There is a formalized procedure for granting and terminating user access to personal data. Users' access is regularly reviewed, including that rights can still be justified by a work-related need. 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that formalized procedures are in place for granting and discontinuing users' access to systems and databases used for the processing of personal data.</p> <p>For the most recently employed employees, we have inspected by random samples that the employees' access to systems where personal data is processed has been approved and that the employees have a work-related need for access.</p> <p>For the most recently resigned employees, we have inspected by random samples that the resigned access to systems and databases has been deactivated or discontinued in time.</p> <p>We have inspected the data processor's annual cycle / procedure for user management and observed that the data processor must regularly assess and approve assigned user accesses.</p> <p>We have inspected that the data processor has assessed and approved user access.</p>	No exceptions noted.

Control Area B			
Control objectives			
Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant processing security.			
No.	Control activity	Tests conducted by BDO	Test result
B.14	<p>Logical access control</p> <ul style="list-style-type: none"> ▶ The data processor has established rules for password requirements that must be followed by everyone with access to personal data. ▶ Access to systems and databases in which personal data is processed and poses a high risk to the data subjects shall, at a minimum, be secured using two-factor authentication. 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that users' access to carry out the processing of personal data is done through passwords that reflect the risk of the processing activity.</p> <p>We have inspected that access to databases containing personal data is secured using two-factor authentication.</p>	No exceptions noted.
B.15	<p>Physical access control</p> <ul style="list-style-type: none"> ▶ Physical access security has been established so that only authorized persons can gain physical access to premises and data centers in which personal data is stored and processed. 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that formalized procedures are in place to ensure that only authorized persons can gain physical access to the data processor's office premises.</p> <p>Upon inquiry, we have been informed that the data processor's personal data is stored with sub-processor/hosting provider Hetzner GMBH.</p>	No exceptions noted.
B.16	<p>Backup and restoration</p> <ul style="list-style-type: none"> ▶ The data processor has established a procedure for backup and re-establishment of data and systems that ensures that relevant systems and data are backed up and stored at another physical location, and that systems and data can be re-established. 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that formalized procedures are in place to ensure backup and restoration of relevant data and systems, and that backups are stored in another physical location.</p> <p>We have inspected that backups of relevant systems and data are made in accordance with the procedure.</p> <p>We have inspected that backups have been restored during the reporting period.</p>	No exceptions noted.

Control Area B			
Control objectives			
<i>Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant processing security.</i>			
No.	Control activity	Tests conducted by BDO	Test result
B.17	Remote workplaces and remote access to systems and data <ul style="list-style-type: none"> ▶ The hard disk on employee computers is encrypted. 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected the data processor's information security policy and observed that it requires the hard drives on employees' devices to be encrypted.</p> <p>On a sample basis we have inspected that employees' hard drives are encrypted.</p>	No exceptions noted.

Control Area C			
Control objectives			
Procedures and controls are complied with to ensure that the data processor has implemented organizational measures to ensure relevant processing security.			
No.	Control activity	Tests conducted by BDO	Test result
C.1	<p>Information security policies and information security policy review</p> <ul style="list-style-type: none"> ▶ The data processor's management has approved a written information security policy, which has been communicated to all relevant stakeholders, including the data processor's employees. The IT security policy is based on the risk assessment carried out. ▶ An assessment is made on an ongoing basis – and at least once a year – of whether the IT security policy needs to be updated. 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that there is an information security policy that the management has processed and approved.</p> <p>We have inspected documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.</p> <p>We have inspected that procedures have been updated and approved during the reporting period.</p>	No exceptions noted.
C.2	<p>Information security policies in accordance with data processing agreements</p> <ul style="list-style-type: none"> ▶ The management of the data processor has ensured that the information security policy is not in conflict with the concluded data processing agreements. 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected documentation of the management's assessment that the information security policy generally meets the requirements for security measures and processing security in the concluded data processing agreements.</p> <p>We have inspected the data processing agreements by a random sample that the requirements in the agreements do not conflict with the information security policy.</p>	No exceptions noted.
C.3	<p>Recruitment of employees – Screening</p> <ul style="list-style-type: none"> ▶ The Data Processor performs screening of potential employees before employment based on the job. 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that there are formalized procedures in place to ensure verification of the data processor's employees in connection with employment.</p>	No exceptions noted.

Control Area C			
Control objectives			
Procedures and controls are complied with to ensure that the data processor has implemented organizational measures to ensure relevant processing security.			
No.	Control activity	Tests conducted by BDO	Test result
		For the most recent employees, we have inspected by random samples that the data processor has carried out a verification of the candidate and that the verification has included relevant documentation.	
C.4	Recruitment of employees - Non-disclosure agreement with employees and introduction to information security <p>▶ Upon employment, employees sign a confidentiality agreement. Furthermore, the employee is introduced to information security policy and procedures regarding data processing as well as other relevant information in connection with the employee's processing of personal data.</p>	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>For the most recently hired employees, we have inspected by random samples that the employees in question have signed a requirement for confidentiality in the employment contract.</p> <p>For the most recently hired employees, we have inspected by random samples that the employees in question have been introduced to:</p> <ul style="list-style-type: none"> • Information security policy • Procedures relating to data processing, as well as other relevant information. 	No exceptions noted.
C.5	Termination of employees - withdrawal of access rights and assets <p>▶ Upon resignation, a process has been implemented by the data processor to ensure that the user's rights become inactive or cease, including that assets are confiscated.</p>	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected procedures that ensure the rights of terminated employees are deactivated or terminated upon termination, and that assets such as access cards, PCs, mobile phones, etc., are revoked.</p> <p>For the most recently terminated employees, we have inspected by random samples that rights have been deactivated or terminated, and that assets have been revoked in a timely manner.</p>	No exceptions noted.

Control Area C			
Control objectives			
Procedures and controls are complied with to ensure that the data processor has implemented organizational measures to ensure relevant processing security.			
No.	Control activity	Tests conducted by BDO	Test result
C.6	<p>Resignation of employees - information about confidentiality and professional secrecy</p> <p>▶ Upon resignation, the employee is informed that the signed confidentiality agreement is still in force and that the employee is subject to a general duty of confidentiality in relation to the processing of personal data that the data processor performs for the data controllers.</p>	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>For the most recently resigned employees, we have inspected by random samples that the data processor has informed the re-signed employees that the imposed duty of confidentiality still applies after termination of employment.</p>	No exceptions noted.
C.7	<p>Awareness, education and training regarding information security</p> <p>▶ Ongoing awareness training is carried out of the data processor's employees in relation to IT security in general and processing security in relation to personal data.</p>	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that the data processor offers awareness training to employees covering general IT security and processing security in relation to personal data.</p> <p>We have inspected documentation that all employees who either have access to or process personal data have completed the awareness training offered.</p>	No exceptions noted.
C.8	<p>Supporter's access to personal data</p> <p>▶ The Data Processor has established procedures for supporters' access to personal data, which ensure that supporters' access and handling of personal data in connection with support tasks is based on support tickets and the supporter's work-related needs.</p>	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that there are formalized procedures in place to ensure that supporters' access and handling of personal data in connection with support tasks is based on support tickets and the supporter's work-related needs.</p> <p>We have inspected a support case by random samples and observed that it follows the procedure.</p>	No exceptions noted.

Control area D			
Control objectives			
<i>Procedures and controls are complied with to ensure that personal data can be deleted or returned if an agreement is entered into with the data controller.</i>			
No.	Control activity	Tests conducted by BDO	Test result
D.1	<p>Deletion of information in accordance with the data controller's requirements</p> <ul style="list-style-type: none"> ▶ There are written procedures that include requirements for the storage and deletion of personal data in accordance with the agreement with the data controller. ▶ Ongoing assessments are conducted – at least once a year – to determine whether the procedures need to be updated. 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that formalized procedures are in place for the storage and deletion of personal data in accordance with the agreement with the data controller.</p> <p>We have inspected that the procedures have been updated and approved during the reporting period.</p>	No exceptions noted.
D.3	<p>Deletion and return upon termination of customer relationship</p> <ul style="list-style-type: none"> ▶ Upon termination of processing of personal data by the Data Controller, data in accordance with the agreement with the Data Controller are: <ul style="list-style-type: none"> • Returned to the Data Controller, and/or • Deleted where it does not conflict with other legislation. 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that there are formalized procedures for the return and/or deletion of the data controller's data upon termination of the processing of personal data.</p> <p>For the most recent terminated data processing, we have inspected by random samples that the agreed deletion of data has been carried out in a timely manner.</p>	No exceptions noted.

Control Area E			
Control objectives			
Procedures and controls are complied with to ensure that the data processor only stores personal data in accordance with the agreement with the data controller.			
No.	Control activity	Tests conducted by BDO	Test result
E.1	<p>Storage of information is in accordance with the data controller's requirements</p> <ul style="list-style-type: none"> ▶ There are written procedures that include requirements for the storage of personal data solely in accordance with the agreement with the data controller. ▶ Ongoing assessments are conducted – at least once a year – to determine whether the procedures need to be updated. 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that there are formalized procedures for only storing and processing personal data in accordance with the data processing agreements.</p> <p>We have inspected that personal data is stored until the customer relations are ended.</p> <p>We have inspected that the procedures have been updated and approved during the reporting period.</p>	No exceptions noted.
E.2	<p>Location of processing and storage of information</p> <ul style="list-style-type: none"> ▶ The data processor's data processing, including storage, may only take place at locations, countries, or territories approved by the data controller. 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that the data processor has a comprehensive and updated overview of processing activities with an indication of locations, countries or areas of land for the processing and storage of personal data.</p> <p>We have inspected by random samples of data processing activities from the data processor's overview of processing activities, and found documentation that data processing, including the storage of personal data, is only carried out at the locations specified in the data processing agreement – or otherwise approved by the data controller.</p>	No exceptions noted.

Control Area F			
Control objectives			
Procedures and controls are complied with to ensure that only approved sub-processors are used, and that the data processor ensures satisfactory processing security when following up on their technical and organizational measures to protect the rights of the data subjects and the processing of personal data.			
No.	Control activity	Tests conducted by BDO	Test result
F.1	Sub-data processing agreement and instructions <ul style="list-style-type: none"> ▶ There are written procedures that contain requirements for the data processor when using sub-processors, including requirements for sub-data processing agreements and instructions. ▶ An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated. 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that there are formalized procedures for the use of sub-processors, including requirements for sub-data processing agreements and instructions.</p> <p>We have inspected that the procedures have been updated and approved during the reporting period.</p>	No exceptions noted.
F.2	Approval of sub-processors <ul style="list-style-type: none"> ▶ The data processor only uses sub-processors for the processing of personal data that has been specifically or generally approved by the data controller. 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that the data processor has a comprehensive and updated overview of the sub-processors used.</p> <p>We have inspected a random sample of sub-processors from the data processor's overview of sub-processors and found documentation that the sub-processor's data processing is included in the most recently concluded data processing agreement with a data controller.</p>	No exceptions noted.
F.3	Changes in approved sub-processors <ul style="list-style-type: none"> ▶ In the event of changes in the use of generally approved sub-processors, the data controller is notified in a timely manner to allow for objections and/or the withdrawal of personal data from the data processor. In the event of changes in the use of specifically approved sub-processors, this is approved by the data controller. 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that there are formalized procedures for notifying the data controller of changes in the use of sub-processors.</p> <p>Upon inquiry, we have been informed that there have been no changes to sub-processors during the reporting period.</p>	<p>We have been informed that there have been no changes to sub-processors. We have therefore not been able to test the control for implementation and effectiveness .</p> <p>No exceptions noted.</p>

Control Area F			
Control objectives			
Procedures and controls are complied with to ensure that only approved sub-processors are used, and that the data processor ensures satisfactory processing security when following up on their technical and organizational measures to protect the rights of the data subjects and the processing of personal data.			
No.	Control activity	Tests conducted by BDO	Test result
F.4	<p>The sub-processor's obligations</p> <p>▶ The data processor has imposed on the sub-processor the same data protection obligations as those provided for in the data processing agreement or similar with the data controller.</p>	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that data processing agreements have been entered into with the sub-processors used,</p> <p>We have inspected a random sample of sub-processor agreements and found that they contain the same requirements and obligations as those stated in the data processing agreements between the data controllers and the data processor.</p>	No exceptions noted.
F.5	<p>Overview of sub-processors</p> <p>▶ The data processor has a list of approved sub-processors stating:</p> <ul style="list-style-type: none"> • Name • CVR no. • Address • Description of the treatment 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that the data processor has a comprehensive and updated overview of used and approved sub-processors.</p> <p>We have inspected that the overview contains at least the required information about the individual sub-processors.</p>	No exceptions noted.
F.6	<p>Supervision of sub-processors</p> <p>▶ Based on an updated risk assessment of each sub-processor and the activities carried out by them, the data processor conducts ongoing follow-up through meetings, inspections, review of audit statements, or similar.</p>	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected documentation that a risk assessment has been carried out for each sub-processor and the current processing activities.</p> <p>We have inspected that the data processor has conducted supervision, including obtaining and reviewing the sub-processor's audit reports, certifications, and similar.</p>	No exceptions noted..

Control Area F			
Control objectives <i>Procedures and controls are complied with to ensure that only approved sub-processors are used, and that the data processor ensures satisfactory processing security when following up on their technical and organizational measures to protect the rights of the data subjects and the processing of personal data.</i>			
No.	Control activity	Tests conducted by BDO	Test result
		We have inspected that the data processor's supervision of sub-processors has not necessitated further actions.	

Control Area H			
Control objectives			
Procedures and controls are complied with to ensure that the data processor can assist the data controller with the disclosure, correction, deletion or restriction of information about the processing of personal data to the data subject.			
No.	Control activity	Tests conducted by BDO	Test result
H.1	<p>Procedure for fulfilling the rights of data subjects</p> <ul style="list-style-type: none"> ▶ There are written procedures that include requirements for the data processor to assist the data controller in relation to the data subjects' rights. ▶ Ongoing assessments are conducted – at least once a year – to determine whether the procedures need to be updated. 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that there are formalized procedures in place for the data processor's assistance of the data controller in relation to the rights of the data subjects.</p> <p>We have inspected that the procedures have been updated and approved.</p>	No exceptions noted.
H.2	<p>Technical measures for the fulfilment of data subjects' rights</p> <ul style="list-style-type: none"> ▶ The data processor has established procedures which, to the extent agreed, enable timely assistance to the data controller in relation to the disclosure, correction, deletion or restriction of, and information about the processing of, personal data to the data subject. 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that the available procedures for assistance to the data controller contain detailed procedures for:</p> <ul style="list-style-type: none"> • Disclosure of information • Correction of information • Deletion of information • Restriction of processing of personal data • Information about the processing of personal data for the data subject. <p>Upon inquiry, we have been informed that no request for assistance has been made in relation to the rights of the subjects.</p>	<p>We have been informed that there has been no request for assistance in relation to the rights of the subjects. We have therefore not been able to test the control for implementation and effectiveness .</p> <p>No exceptions noted.</p>

Control Area I			
Control objectives			
Procedures and controls are complied with to ensure that any security breaches can be handled in accordance with the data processing agreement.			
No.	Control activity	Tests conducted by BDO	Test result
I.1	<p>Notification of personal data breaches</p> <ul style="list-style-type: none"> ▶ There are written procedures that require the data processor to notify the data controllers in the event of a personal data breach. ▶ Ongoing assessments are conducted – at least once a year – to determine whether the procedures need to be updated. 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that there are formalized procedures that contain requirements for notifying the data controllers in the event of a personal data breach.</p> <p>We have inspected that the procedure has been updated and approved during the reporting period.</p>	No exceptions noted.
I.2	<p>Identification of personal data breaches</p> <ul style="list-style-type: none"> ▶ The Data Processor has established the following controls for the identification of any personal data breaches: <ul style="list-style-type: none"> • Awareness among employees • Network traffic monitoring • Follow-up on logging access to personal data 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that the data processor provides awareness training to employees in relation to the identification of any personal data breaches.</p> <p>We have inspected documentation that network traffic is monitored, as well as that there is follow-up on abnormalities, surveillance alarms, transfer of large files, etc.</p> <p>We have inspected documentation to ensure that there is timely follow-up on logging of access to personal data, including follow-up on repeated attempts at access.</p>	No exceptions noted.
I.3	<p>Timely notification of personal data breaches</p> <ul style="list-style-type: none"> ▶ In the event of any breaches of personal data security, the data processor has notified the data controller without undue delay and no later than 48 hours after becoming aware of a breach of personal data security at the data processor or a sub-processor 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that the data processor has an overview of security incidents with an indication of whether the individual incident has resulted in a breach of personal data security.</p>	<p>We have been informed that no incidents have been identified that have led to a breach of personal data security. We have therefore not been able to test the control for implementation and effectiveness .</p> <p>No exceptions noted.</p>

Control Area I			
Control objectives			
Procedures and controls are complied with to ensure that any security breaches can be handled in accordance with the data processing agreement.			
No.	Control activity	Tests conducted by BDO	Test result
		We have observed that no incidents have been found that have led to a breach of personal data security during the reporting period.	
I.4	<p>Assistance to data controllers in the event of a personal data breach</p> <p>▶ The data processor has established procedures for assistance to the data controller in its notification to the Danish Data Protection Agency:</p> <ul style="list-style-type: none"> • The nature of the personal data breach • Likely consequences of the personal data breach • Measures that have been taken or are proposed to be taken to deal with the personal data breach. 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that the procedures available for notifying data controllers in the event of a personal data breach contain detailed procedures for:</p> <ul style="list-style-type: none"> • Description of the nature of the personal data breach • Description of the likely consequences of the personal data breach • Description of measures taken or proposed to be taken to deal with the personal data breach. <p>We have observed that no incidents have been found that have led to a breach of personal data security during the reporting period.</p>	<p>We have been informed that no data breach has led to assistance to the data controllers during the reporting period. We have therefore not been able to test the control for implementation and effectiveness .</p> <p>No exceptions noted.</p>

Control area J			
Control objectives <i>Procedures and controls are complied with that ensure information security and data protection are planned and implemented in the data processor's development and change process.</i>			
No.	Control activity	Tests conducted by BDO	Test result
J.1	<p>Change management and privacy-by-design</p> <p>▶ The data processor has established a procedure for development and change tasks that ensures compliance with the privacy-by-design principles, and that all development and change tasks follow a formalized process that ensures testing and requirements for approval before implementation.</p>	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that the data processor has established a procedure for development and change tasks that ensures compliance with privacy-by-design principles, and that all development and change tasks follow a formalized process that ensures testing and approval requirements before implementation.</p> <p>For the most recently implemented changes/developments, we have inspected by samples that the developments/changes task has ensured compliance with privacy-by-design principles.</p> <p>We have also inspected that the task followed the formalized process, and that testing was conducted, and the change/development was approved before implementation.</p>	No exceptions noted.
J.2	<p>Implementing change in the production environment</p> <p>▶ The data processor has established a procedure for implementing changes in the production environment that ensures separation of functions in the implementation process.</p>	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that there is a segregation of duties so that developers cannot implement changes directly in the production environment.</p>	No exceptions noted.
J.3	<p>Separation of the development, test, and production environment</p> <p>▶ Development and testing are performed in development environments that are separate from production environments.</p>	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that the development, testing and production environment are separated.</p>	No exceptions noted.

Control area J			
Control objectives			
<i>Procedures and controls are complied with that ensure information security and data protection are planned and implemented in the data processor's development and change process.</i>			
No.	Control activity	Tests conducted by BDO	Test result
J.4	<p>Access to source code</p> <ul style="list-style-type: none"> ▶ Source code is protected from unauthorized modification and deletion. 	<p>We have conducted inquiries with appropriate personnel of the data processor.</p> <p>We have inspected that only the data processor's developers have access to source code.</p> <p>We have inspected documentation that the source code is protected against unauthorized modification and deletion.</p>	No exceptions noted.

**BDO STATSATORISERET
REVISIONSPARTNERSELSKAB**

**VESTRE RINGGADE 28
8000 AARHUS C**

www.bdo.dk

BDO Statsautoriseret Revisionspartnerselskab, a Danish-owned advisory and auditing firm, is a member of BDO International Limited - a UK-based company with limited liability - and part of the international BDO network consisting of independent member firms. BDO is the trademark of both the BDO network and of all BDO member firms. BDO in Denmark employs more than 1,800 people, while the worldwide BDO network has approx. 120,000 employees in more than 166 countries.

*Copyright - BDO Statsautoriseret Revisionspartnerselskab,
cvr.nr. 45719375.*



PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registreret, og informationerne er listet herunder.

“Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument.”

Mikkel Jon Larsen

BDO Statsautoriseret Revisionspartnerselskab CVR: 45719375
Partner

Serienummer: cd9a38dd-e75c-40f7-80d6-ec5b5d0841d6
IP: 77.215.xxx.xxx
2025-11-03 11:35:47 UTC



Nicolai Tobias Visti Pedersen

BDO Statsautoriseret Revisionspartnerselskab CVR: 45719375
Statsautoriseret revisor

Serienummer: c42f66e9-59bb-478a-9d92-2a2b8602724e
IP: 37.96.xxx.xxx
2025-11-03 13:35:28 UTC



Jacob Martin Barlach

CTO og Chefudvikler

Serienummer: 63a7b013-50b5-4470-b3cd-1797a4659b34
IP: 80.208.xxx.xxx
2025-11-03 16:35:41 UTC



Dette dokument er underskrevet digitalt via [Penneo.com](https://penneo.com). De underskrevne data er valideret vha. den matematiske hashværdi af det originale dokument. Alle kryptografiske beviser er indlejret i denne PDF for validering i fremtiden.

Dette dokument er forseglet med et kvalificeret elektronisk segl. For mere information om Penneos kvalificerede tillidstjenester, se <https://eutl.penneo.com>.

Sådan kan du verificere, at dokumentet er originalt

Når du åbner dokumentet i Adobe Reader, kan du se, at det er certificeret af **Penneo A/S**. Dette beviser, at indholdet af dokumentet er uændret siden underskriftstidspunktet. Bevis for de individuelle underskrivers digitale underskrifter er vedhæftet dokumentet.

Du kan verificere de kryptografiske beviser vha. Penneos validator, <https://penneo.com/validator>, eller andre valideringstjenester for digitale underskrifter.