GAPSOLUTIONS A/S

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT FROM 1. OCTOBER 2022 TO 30. SEPTEMBER 2023 ON THE DESCRIPTION OF SAAS SOLUTIONS GRC PORTAL AND WHISTLEBLOWER SCHEME AND RELATED TECHNICAL AND ORGANISATIONAL MEASURES AND OTHER CONTROLS AND THEIR DESIGN RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DATA PROTECTION LAW.

CONTENTS

1. INDEPENDENT AUDITOR'S REPORT 2

2. GAPSOLUTION A/S' STATEMENT 5

3. GAPSOLUTION A/S' DESCRIPTION OF THE SAAS SOLUTIONS GRC PORTAL AND WHISTLEBLOWER SCHEME 7

GapSolution A/S 7

SaaS Solutions GRC Portal And Whistleblower Scheme and Processing Of Personal Data 7

Management of the security of personal data 7

Risk Assessment 9

Technical and Organisational Security Measures and Other Controls 10

Changes from 1 October 2022 To 30 September 2023 13

Complementary Controls for Data Controllers 13

4. CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND THE RESULT OF TESTS 14

Control area A 16

Control area B 19

Control area C 28

Control area D 33

Control area E 34

Control area F 35

Control area H 38

Control area I 39

1. INDEPENDENT AUDITOR'S REPORT

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT 1. OCTOBER 2022 TO 30. SEPTEMBER 2023 ON THE DESCRIPTION OF SAAS SOLUTIONS GDPR-PORTAL AND WHISTLEBLOWER SCHEME AND RELATED TECHNICAL AND ORGANISATIONAL MEASURES AND OTHER CONTROLS AND THEIR DESIGN AND OPERATING EFFECTIVENESS RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DANISH ACT ON SUPPLEMENTARY PROVISIONS

To: The Management of GapSolutions A/S
GapSolutions A/S Customers

Scope

We have been engaged to report on GapSolution A/S' (the Data Processor) description in section 3 of SaaS solutions GRC Portal and Whistleblower scheme and the related technical and organisational measures and other controls, relating to 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 with regard to the processing of personal data and on the free movement of such data (the EU General Data Protection Regulation) and the Danish Act on Supplementary Provisions to the Regulation (Danish Data Protection Act), and on the design and operating effectiveness of the technical and organisational measures and other controls related to the control objectives stated in the description for the period 1. October 2022 to 30. September 2023.

The Data Processor's Responsibilities

The Data Processor is responsible for preparing the statement in section 2 and the accompanying description including the completeness, accuracy, and method of presenting the statement and the description. Furthermore, the Data Processor is responsible for providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Auditor's Independence and Quality Control

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

BDO Statsautoriseret revisionsaktieselskab applies International Standard on Quality Management, ISQM 1, which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's Responsibilities

Our responsibility is to express an opinion on the Data Processor's description in section 3 and on the design and operating effectiveness of the controls related to the control objectives stated in the description, based on our procedures.

We conducted our engagement in accordance with the International Standard on Assurance Engagements 3000, "Reports Other Than Audits or Reviews of Historical Financial Information". That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are appropriately designed.

An assurance engagement to report on the description, design and operating effectiveness of controls at a Data Processor involves performing procedures to obtain evidence about the disclosures in the Data Processor's description and about the design and operating effectiveness of the controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks that the description is not fairly presented, and that controls are not appropriately designed or operating effectively. Our procedures included evaluating the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the appropriateness of the objectives stated therein, and the suitability of the criteria specified by the Data Processor and described in section 2.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

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 may not, therefore, include every aspect of the use of SaaS solutions GRC Portal and Whistleblower scheme, that each individual Controller may consider important in their own environment. Also, because of their nature, controls at a Data Processor may not prevent or detect all breaches of the personal data security. Furthermore, the projection of any evaluation of the operating effectiveness of controls to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the Data Processor's statement in section 2. In our opinion, in all material respects:

a. The description presents fairly SaaS solutions GRC Portal and Whistleblower scheme and the related technical and organisational measures and other controls, relating to processing and protection of personal data in accordance with the EU General Data Protection Regulation and the Danish Data Protection Act, as designed and implemented for the period 1. October 2022 to 30. September 2023.

b. The technical and organisational measures and other controls, relating to the control objectives stated in the description were appropriately designed for the period 1. October 2022 to 30. September 2023

c. The technical and organisational measures and other controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period from 1. October 2022 to 30. September 2023.

Description of Test of Controls

The specific controls tested, and the results of those tests are listed in section 4.

Intended Users and Purpose

This report is intended solely for data controllers who have used SaaS solutions GRC Portal and Whistleblower scheme, and who have a sufficient understanding to consider it along with other information, including information about the technical and organisational measures and other controls operated by the data controllers themselves when assessing whether the requirements of the EU General Data Protection Regulation and the Danish Data Protection Act have been complied with.

Copenhagen, 24 November 2023

BDO Statsautoriseret Revisionsaktieselskab

Claus Bonde Hansen
State Authorised Public Accountant

Mikkel Jon Larsen
Partner, chef for Risk Assurance, CISA, CRISC

2. GAPSOLUTION A/S' STATEMENT

GapSolution A/S processes personal data in relation to SaaS solutions GRC Portal and Whistleblower scheme and GapSolution A/S to our customers, who are Data Controllers according to 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 EU General Data Protection Regulation) and the Danish Act on Supplementary Provisions (the Danish Data Protection Act).

The description has been prepared for Data Controllers who have used SaaS solutions GRC Portal and Whistleblower scheme, and who have a sufficient understanding to consider the description along with other information, including information about the technical and organisational measures and other controls operated by the data controllers themselves in assessing whether the requirements of the EU General Data Protection Regulation and the Danish Data Protection Act have been complied with.

Company Name uses sub-processors. These sub-processor's relevant control objectives and related technical and organisational measures and other controls are not included in the accompanying description.

GapSolution A/S confirms that the accompanying description in section 3 fairly presents SaaS solutions GRC Portal and Whistleblower scheme and the related technical and organisational measures and other controls 1. October 2022 to 30. September 2023. The criteria used in making this statement were that the accompanying description:

1. Presents SaaS solutions GRC Portal and Whistleblower scheme, and how the related technical and organisational measures and other controls were designed and implemented, including:
    - 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 GRC Portal 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 on changes in SaaS solutions GRC Portal and Whistleblower scheme and the related technical and organisational measures and other controls throughout the period.

3. Does not omit or distort information relevant to the scope of SaaS solutions GRC Portal and Whistleblower scheme and the related technical and organisational measures and other controls described while acknowledging that this description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of SaaS solutions GRC Portal and Whistleblower scheme that the individual data controllers might consider important in their environment.

GapSolution A/S confirms that the technical and organisational measures and other controls related to the control objectives stated in the accompanying description were suitable designed for the period 1 October 2022 to 30 September 2023. The criteria we used in making this statement were that:

1. The risks threatening achievement of the described control objectives were identified.

2. The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.

3. The controls were applied consistently as designed, including manual controls were performed by persons with appropriate competencies and rights, in the entire period from 1. October 2022 to 30. September 2023.

GapSolution A/S confirms that appropriate technical and organisational measures and other controls were implemented and maintained to comply with the agreements with data controllers, good practices for the data processing of data and relevant requirements for Data Processors in accordance with the EU General Data Protection Regulation and the Danish Data Protection Act.

Horsens, 24 November 2023

GapSolutions A/S

Jacob Barlach
Partner, IT & Marketing

3. GAPSOLUTION A/S' DESCRIPTION OF THE SAAS SOLUTIONS GRC PORTAL AND WHISTLEBLOWER SCHEME

GAPSOLUTION 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 30 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 GRC PORTAL AND WHISTLEBLOWER SCHEME AND PROCESSING OF PERSONAL DATA

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

The GRC Portal 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 the GRC Portal 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.

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:

THE DATA PROCESSING AGREEMENT	CONTROL AREA	ARTICLE
Control area A Procedures and controls are complied with to ensure that instructions regarding the processing of personal data are complied with in accordance with the incoming data processor agreement.	• Entering into a data processing agreement with the Controller • Instruction for processing of personal data • Compliance with instruction for processing of personal data • Communication of unlawful instruction to the controller	• Art. 28 (3) • Art. 28 (3)(a) • Art. 29 • Art. 32 (4) • Art. 28 (10) • Art. 28 (3)(h)
Control area B Procedures and controls are followed, which ensure that the data processor has implemented technical measures to ensure relevant processing security.	• Risk Assessment • Contingency plans in case of physical or technical incidents • Physical access control • Logical access control • Remote workplaces and remote access to systems and data • External communication connections • Encryption of personal data • Firewall • Network security • Anti-virus program • Back-up and re-establishment of data • Maintenance of system software • Logging in systems, databases, and network, including logging of application of personal data. • Monitoring • Testing, assessment, and evaluation of the efficiency of the technical and organisational security measures • Information security in development and changes • Segregation of development, test, and production environments • Personal data in development and test environments • Support assignments	• Art. 28 (3)(c) • Art. 25
Control area C Procedures and controls are followed, which ensure that the data processor has implemented organizational measures to ensure relevant processing security.	• Information Security Policy • Review of the information security policy • Organization of information security policy • Recruitment of employees • Resignation of employees • Training and instruction of employees processing personal data. • Awareness and information campaigns for employees • Confidentiality and secrecy agreement with employees • Obligations of security of processing and impact assessments. • Audit and inspection • Records of processing activities • Storage of the record • The Danish Data Protection Agency's access to the record • Selection of Data protection officer	• Art. 28(1) • Art. 28 (3)(b) • Art. 28 (3)(f) • Art. 28 (3)(h) • Art. 30 (2), (3) and (4) • Art. 33 (2) and (5) • Art. 38 • Art. 39

THE DATA PROCESSING AGREEMENT	CONTROL AREA	ARTICLE
	• The position of the Data protection office • Tasks of the Data protection officer	
Control area D Procedures and controls are followed, which ensure that personal data can be deleted or returned if an agreement is entered into with the data controller.	• Deletion of personal information • Return of personal information	• Art. 28 (3)(g)
Control area E Procedures and controls are followed, which ensure that the data processor only stores personal data in accordance with the agreement with the data controller.	• Storage of personal data • Handling of input and output data materials	• Art. 28 (3)(c)
Control area F Procedures and controls are followed, which ensure that only approved sub-data processors are used, and that the data processor, by following up on their technical and organizational measures to protect the data subjects' rights and the processing of personal data, ensures satisfactory processing security.	• Sub data processor agreement and instruction • Approval of sub data processors • Changes to approved sub data processors • Overview of approved sub data processors • Supervision of sub data processors	• Art. 28 (2) and (4)
Control area G Procedures and controls are followed to ensure that the data processor only transfers personal data to third countries or international organizations in accordance with the agreement with the data controller on the basis of a valid transfer basis.	• The data subjects' rights • Instructions from the data controller • Valid transfer basis	• Art. 44 - 49
Control area H Procedures and controls are followed, which ensure that the data processor can assist the data controller with the provision, correction, deletion or restriction of information on the processing of personal data to the data subject.	• The data subject's rights	• Art. 28 (3)(e)
Control area I Procedures and controls are followed to ensure that any security breaches can be managed in accordance with the data processor agreement entered into.	• Notification of personal data breaches • Assistance to the data controller in relation to personal data breaches	• Art. 33 (2) • Art. 28 (3)(f)

RISK ASSESSMENT

Management is responsible for initiating all initiatives that counteract the threat landscape 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 the 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.

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 about the use of sub-processors. The data processing agreements become effective when the order confirmation with the associated and conditions of sale and delivery is signed by both parties. This is stored electronically.

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.

Technical and organisational security measures

Risk Assessment

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

Contingency Plans

GapSolutions A/S has established contingency plans so that GapSolutions A/S can restore the availability of and access to personal data in the event of physical or technical incidents promptly. GapSolutions A/S has established a crisis response team that comes into play in these cases.

Organization of the crisis response group has been established, and guidelines for activating the crisis response are in place. GapSolutions A/S has developed detailed contingency plans and guidelines for system and data restoration, ensuring personal independence in connection with the activation of the emergency response and restoration. The plans are regularly evaluated and revised to ensure that they are up-to-date and effective in critical situations.

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.

The physical security of GapSolutions A/S' servers is described in more detail in the data processing agreement with Hetzner GMBH. The physical security of sub-processors that process data as part of GapSolutions A/S' processing on behalf of the data controller is described in the data processing agreement with each sub-processor.

Logical Access Security

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.

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.

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.

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.

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.

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.

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.

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.

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

Testing, Assessment, and Evaluation
GapSolutions A/S has implemented procedures for regular testing, assessment, and evaluation of the effectiveness of technical and organizational security measures to ensure data processing security.

Data Protection by Design and Default
GapSolutions A/S has implemented policies and procedures for the development and maintenance of the GRC portal 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.

Data Processor's Assurances
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 Legal Duty of Secrecy
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.

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 35regarding impact assessments.

Assistance to the Data Controller Regarding Audit and Inspection
GapSolutions A/S has implemented policies and procedures to ensure that GapSolutions A/S can provide all necessary information to demonstrate compliance with the requirements of the data processor to the data controller. GapSolutions A/S also allows and contributes to audits, including inspections, conducted by the data controller or others authorized by the data controller.

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.

Deletion 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.

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
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.

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.

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 Article 33 on the notification and communication of personal data breaches.

CHANGES FROM 1 OCTOBER 2022 TO 30 SEPTEMBER 2023

GapSolutions A/S has not made significant changes to the SaaS solutions GRC Portal and Whistleblower scheme and their associated technical and organizational security measures and other controls from October 1, 2022, to September 30, 2023.

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 GRC Portal 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 GRC Portal and Whistleblower scheme, including which individuals are granted administrator access and what rights individual administrators are assigned.

- The data controller may not use the GRC Portal 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 GRC Portal and Whistleblower scheme.

4. CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND THE RESULT OF TESTS

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

BDO has inspected procedures to obtain evidence of the information in GapSolution A/S' description of SaaS solutions GRC Portal and Whistleblower scheme, the design and operating effectiveness of the relating technical and organisational measures and other controls. The procedures selected depend on BDO's assessment, including the assessment of the risks that the description is not fairly presented and that the controls are not appropriately designed or operating effectively.

BDO's test of the design and the operating effectiveness of the relating technical and organisational measures and other controls and their implementation has included the control objectives and related the control objectives and related control activities selected by GapSolution A/S, and which are described in the check form below.

In the test form, BDO has described the tests carried out which were assessed necessary to obtain reasonable assurance that the stated control objectives were achieved, and that related controls were appropriately designed and operated effectively for the period 1. October 2022 to 30 September 2023.

Test procedures

Test of the design of the relating technical and organisational measures and other controls and their implementation was performed by inquiries, inspection, observation and re-performance.

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.

With respect to the services provided by Hetzner GMBH within hosting, we have from independent auditor 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 October 1, 2022, To September 30, 2023.

With respect to the services provided by Flowmailer B.V within the mail service, we have from independent auditor received valid ISO 27001 certification for the sub data providers' technical and organisational security measures and other controls.

With respect to the services provided by Timbet within scanning of the WB portal, we have received the data processor's GDPR supervision of the sub processor's technical and organisational security measures and other controls.

These sub-processor's relevant control objectives and related controls of the sub-processor are not included in GapSolutions A/S´ description of SaaS solutions GDPR-Portal and Whistleblower scheme and relevant controls related to operation of SaaS solutions GDPR-Portal and Whistleblower scheme. Thus, we have solely assessed the reports and tested the controls at GapSolutions A/S, which ensures appropriate supervision of the sub-processor's compliance with the data processing agreement made between the sub-processor and the data processor and compliance with the General Data Protection Regulation and the Danish Data Protection Act.

Result of test

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

An exception exists when:

- Technical and organisational measures and other controls have not been designed or implemented to fulfil a control objective, and
- Technical and organisational 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 Objective ▶ *Procedures and controls are followed to ensure that instructions regarding the processing of personal data are complied with in accordance with the data processing agreement entered into.*		
Control activities	**Test performed by BDO**	**Result of test**
Entering into a data processing agreement with the Controller ▶ The Data Processor has procedures for entering into written data processing agreements which are in accordance with the services provided by the Data Processor. ▶ The Data Processor applies a data processing agreement template for entering into data processor agreements. ▶ When entering a written data processing agreement based on the data controllers' template, the data processor uses a checklist to ensure that it can comply with the data processing agreement. ▶ Data processing agreements are signed and stored electronically. ▶ Data processing agreements contain information about the use of sub processors.	We have made inquiries with the appropriate personnel at the data processor. We have inspected the data processor's privacy policy and observed that the data processor has implemented procedures for entering into data processing agreements to ensure that the data processor enters into a data processing agreement specifying the terms for processing personal data on behalf of the data controller. We have inspected the data processor's data processing templates regarding the GDPR portal and Whistleblower scheme. We have inspected both templates and observed that they are based on the Data Inspection Authority's template and contain information regarding the use of sub-processors. On a sample basis we have inspected data processing agreements for the GDPR portal and observed that the data processing agreements are signed, electronically stored, and contain information about the use of sub-processors. On a sample basis we have inspected data processing agreements for the Whistleblower scheme and observed that the data processing agreements are signed, electronically stored, and contain information about the use of sub-processors.	No exceptions noted.
Instruction for processing of personal data ▶ Data processing agreement contains instructions from data controller(s). ▶ The Data Processor obtains instruction for processing personal data from the Controller, in connection with entering into a data processor agreement.	We have made inquiries with the appropriate personnel at the data processor. We have inspected the data processor's privacy policy and observed that the data processor has implemented procedures for	No exceptions noted.

Control area A		
Control Objective ▶ *Procedures and controls are followed to ensure that instructions regarding the processing of personal data are complied with in accordance with the data processing agreement entered into.*		
Control activities	**Test performed by BDO**	**Result of test**
	entering into data processing agreements that ensure that processing of personal data only occurs when there is an instruction. On a sample basis we have inspected an executed data processing agreement for the GDPR portal and observed that the data processing agreement includes an instruction from the data controller. On a sample basis we have inspected data processing agreements for the Whistleblower scheme and observed that the data processing agreements include an instruction from the data controller.	
Compliance with instruction for processing of personal data ▶ The data processor only carries out the processing of personal data that appears in instructions from the data controller. ▶ The data processor carries out self-monitoring of compliance with instructions in concluded data processing agreements.	We have made inquiries with the appropriate personnel at the data processor. We have inspected the data processor's privacy policy and observed that the data processor has implemented procedures for entering into data processing agreements that ensure that processing of personal data only occurs when there is an instruction. On a sample basis we have inspected an executed data processing agreement for the GDPR portal and observed that the data processing agreement includes an instruction from the data controller. On a sample basis we have inspected data processing agreements for the Whistleblower scheme and observed that the data processing agreements include an instruction from the data controller.	No exceptions noted.

Control area A

Control Objective

- *Procedures and controls are followed to ensure that instructions regarding the processing of personal data are complied with in accordance with the data processing agreement entered into.*

Control activities	Test performed by BDO	Result of test
Communication of unlawful instruction to the Controller ▶ The Data Processor has prepared a procedure for communication to the Controller when the Controller's instruction is in contravention of the data protection legislation. ▶ The Data Processor communicates immediately to the Controller, if the Controller's instruction is in contravention of the data protection legislation.	We have made inquiries with appropriate personnel at the data processor. On a sample basis we have inspected data processing agreements and observed that the data processor is obligated to inform the data controller if an instruction, in the data processor's opinion, is in violation of the Data Protection Regulation or data protection provisions in other EU law or national law of member states. We have been informed that there have been no incidents related to illegal instructions at the conclusion of the audit. Therefore, we have not evaluated the procedure for implementation and effectiveness in the declaration period.	No exceptions noted.

Control area B

Control Objective

- *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*

Control activities	Test performed by BDO	Result of test
Risk Assessment ▶ The data processor has carried out a risk assessment and, based on this, implemented the technical security measures that have been assessed as relevant to achieve adequate security, including establishing the security measures agreed with the data controller. ▶ The risk assessment is carried out continuously and at least once a year.	We have made inquiries with appropriate personnel at the data processor. We have inspected the data processor's risk assessment and observed that the data processor has assessed a range of risks related to the offered solutions. We have observed that the data processor has mitigated risks through technical measures in relation to identified risks, thus reducing the risks to an acceptable level. On a sample basis we have inspected that the data processor has implemented the technical measures for risk minimization. We have observed that there is a control in place for the annual review of the risk assessment. We have observed that risk assessment has been updated during the declaration period.	No exceptions noted.
Contingency plans in case of physical or technical incidents ▶ The Data Processor has established a contingency plan, which ensures quick response time to restore the accessibility of and access to personal data in a timely manner, in case of a physical or technical incident. ▶ The Data Processor has established periodic testing of the contingency plan with a view to ensure that the contingency plans are up-to-date and efficient in critical situations. ▶ Tests of the contingency plans are documented and evaluated.	We have made inquiries with appropriate personnel at the data processor. We have inspected the data processor's contingency plan, which is designed to ensure that the data processor can promptly restore the availability and access to personal data in the event of physical or technical incidents. We have observed that there is a control in place for conducting semi-annual testing of the contingency plan. On a sample basis we have inspected the most recent test of the contingency plan.	No exceptions noted.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
Physical access control ▶ The data processor has introduced procedures that ensure that premises are protected against unauthorized access. Only persons 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. ▶ Physical access security has been established so that only authorized persons can gain physical access to premises where personal information is processed.	We have made inquiries with appropriate personnel at the data processor. We have inspected that the data processor has a procedure for visitors to the office and observed that visitors must be accompanied. We have observed that locks are installed on all exterior doors of the data processor's office building, and visitors are accompanied. We have been informed that the data processor has outsourced the operation of servers and databases where personal data is stored and processed to the hosting provider Hetzner GMBH. We have inspected data processing agreement between the data processor and the hosting provider and observed that an agreement for the operation of servers and databases has been made. We have inspected the ISO 27001 certification of Hetzner GMBH. We have inspected the security report regarding the technical and organizational measures of Hetzner GMBH.	No exceptions noted.
Logical access control ▶ Access to personal data is isolated to users with a work-related need for this. ▶ A business procedure has been introduced for granting and terminating user access to personal information. ▶ A periodic review of users and their associated rights is conducted.	We have made inquiries with appropriate personnel at the data processor. We have been informed that when new employees start, the management of the data processor assigns permissions to the employees based on job-related needs.	No exceptions noted.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
▶ Multi-factor authentication is used.	We have inspected a list of employees with access to personal data in relevant systems and have confirmed that all users have job-related needs for access and permissions. We have observed that there is a semi-annual control in place to review users and their associated permissions. We have inspected documentation for the most recent user review. On a sample basis we have inspected that access to systems where personal data is processed is protected with multi-factor authentication.	
Remote workplaces and remote access to systems and data ▶ The hard disk on employee computers is encrypted.	We have made inquiries with appropriate personnel at the data processor. We have inspected the data processor's information security policy and observed that it requires the hard drives on employees' devices to be encrypted. On a sample basis we have inspected that employees' hard drives are encrypted.	No exceptions noted.
External communication connections ▶ The data processor has introduced that external communication connections are secured with strong encryption, and e-mail and other communications containing sensitive personal data are encrypted in the shipment.	We have made inquiries with appropriate personnel at the data processor. In the data processor's information security policy, we have inspected the requirement for email encryption via TLS encryption. We have inspected documentation regarding the use of TLS 1.2 encryption.	No exceptions noted.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
	We have inspected documentation for encryption during transmission over the internet and observed that SSL encryption is in place.	
Firewall ▶ External access to systems and databases that are used for processing personal data takes place through a secured firewall.	We have made inquiries with appropriate personnel at the data processor. We have inspected that external access to systems and databases used for the processing of personal data is achieved through secure firewalls. On a sample basis we have inspected that firewalls are enabled laptops. We have inspected the executed 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 the operation and configuration of firewalls. We have inspected Hetzner GMBH's ISO 27001 certification. We have inspected the security report regarding Hetzner GMBH's technical and organizational measures.	No exceptions noted.
Network security ▶ Internal networks are segmented, where traffic between the individual virtual networks is controlled by the firewall.	We have made inquiries with appropriate personnel at the data processor. We have inspected that internal networks are segmented, and the traffic between the individual virtual networks is controlled through firewalls.	No exceptions noted.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
Anti-virus program ▶ Anti-virus software is installed on all servers and workstations. ▶ Anti-virus software is updated on an ongoing basis and updated with the latest version.	We have made inquiries with appropriate personnel at the data processor. On a sample basis we have inspected that antivirus software is installed on laptops and observed that the virus signature was adequately updated. 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. We have inspected Hetzner GMBH's ISO 27001 certification. We have inspected the security report on Hetzner GMBH's technical and organizational measures.	No exceptions noted.
Back-up and re-establishment of data ▶ Back-up of systems and data is performed daily. ▶ Operation and storage of back-ups are outsourced to sub data processor. ▶ Restore test is performed once a year.	We have made inquiries with appropriate personnel at the data processor. We have been informed that the operation and storage of back-ups are outsourced to Hetzner GMBH. We have inspected that Hetzner GMBH conducts daily backups. We have inspected Hetzner GMBH's ISO 27001 certification. We have inspected the security report on Hetzner GMBH's technical and organizational measures. We have inspected that the data processor has established controls for annual restore tests.	No exceptions noted.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
	We have inspected the data processor's most recent performed restore test.	
Maintenance of system software ▶ The Data Processor keeps and overview of operating system software/ third party programmes on work-stations and servers which is updated continuously. ▶ Operating system software on servers and work-stations is constantly updated. ▶ The data processor has implemented a system soft-ware update process to ensure system availability and security.	We have made inquiries with appropriate personnel at the data processor. We have inspected the data processor's information security policy and observed that it is the responsibility of the employ-ees to maintain system software on mobile devices. On a sample basis we have inspected that system software is updated on laptops. 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.	No exceptions noted.
Logging in systems, databases, and network, including logging of application of personal data. ▶ Logging has been established in systems, databases and networks of the following matters: ○ Activities carried out by the user in the data trader's systems. ○ Change in system rights for users. ▶ Log information is protected against manipulation and technical errors and is reviewed as needed.	We have made inquiries with appropriate personnel at the data processor. We have inspected documentation to ensure that all activities within the data processor's system are logged. We have inspected documentation to ensure that changes in system permissions are logged. We have been informed that the data processor's employees do not have the ability to deactivate logging. We have been informed that the log is reviewed as needed or upon request from customers.	No exceptions noted.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
Monitoring ▶ The Data Processor has established a monitor system for monitoring of production environments, including uptime, performance, and capacity. ▶ The Data Processor is notified of identified alerts and follows up on these.	We have made inquiries with appropriate personnel at the data processor. We have been informed that the data processor uses Sentry for system monitoring. We have inspected that alerts from Sentry are sent directly to relevant employees at GapSolution by email.	No exceptions noted.
Testing, assessment, and evaluation of the efficiency of the technical and organisational security measures ▶ The Data Processor tests, assesses, and evaluates the efficiency of whether the technical and organisational security measures are appropriate in relation to the data handled on behalf of the Controller.	We have made inquiries with appropriate personnel at the data processor. We have inspected that controls are in place for testing, assessing, and evaluating the effectiveness of technical and organizational security measures. We have inspected that the data processor's management has approved and reviewed the ISMS (Information Security Management System) and initiated action plans and projects to achieve an adequate level.	No exceptions noted.
Development and maintenance of systems ▶ The data processor has procedures for system development, testing and deployment, that comply with "Privacy by design" and "Privacy by default" principles. ▶ Risk assessment of system changes to ensure data protection through design, cf. Article 25, subsection 1. ▶ Every system change is tested before commissioning. ▶ All system changes are recorded in a change log.	We have made inquiries with appropriate personnel at the data processor. We have inspected the data processor's procedure for system development, testing, and deployment and observed that principles for "Privacy by design" and "Privacy by default" is stated.	No exceptions noted

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
▶ Version control of system changes makes it possible to revert changes in case of errors or the like.	We have inspected that system changes are assessed for risk during task creation. We have inspected that all system changes are recorded and tested. We have inspected that version control of system changes allows for the rollback of changes in case of errors or similar issues.	
Segregation of development, test, and production environments ▶ Segregation of duties between development, test and operation has been introduced.	We have made inquiries with appropriate personnel at the data processor. We have inspected that there is functional separation between system development, testing, and production environments.	No exceptions noted.
Personal data in development and test environments ▶ Fictional test data or anonymised data are used in development and test environments.	We have made inquiries with appropriate personnel at the data processor. We have been informed that the data processor uses a program that generates fake data for development purposes. We have inspected that the system is used to generate fake data. We have inspected that customer data is not used in the test and development environment.	No exceptions noted.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
Support assignments ▶ Supporters access and handling of personal data is given based on support tickets and the supports work related need.	We have made inquiries with appropriate personnel at the data processor. We have inspected a list of employees with access to support in relevant systems. Upon enquiry, we have been informed that that all users listed have job-related needs for the access. We have inspected documentation for the most recent user review.	No exceptions noted.

Control area C		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
Information Security Policy ▶ The Data Processor has prepared and implemented an information security policy. ▶ The information security policy is communicated to all employees.	We have made inquiries with appropriate personnel at the data processor. We have inspected that the data processor has a management-approved information security policy. We have inspected that all employees have sign-off on that they have read the information security policy.	No exceptions noted.
Review of the information security policy ▶ The Data Processor's information security policy is re-viewed and updated at least once annually.	We have made inquiries with appropriate personnel at the data processor. We have inspected that there is a control in place for the an-nual review and approval of the information security policy. We have inspected that the information security policy has been reviewed and approved during the declaration period.	No exceptions noted.
Organisation of information security policy ▶ The Data Processor has defined and established or-ganization of personal data security.	We have made inquiries with appropriate personnel at the data processor. We have inspected that the data processor has described and established the organization of personal data security within the company.	No exceptions noted.
Recruitment of employees ▶ The Data Processor performs screening of potential employees before employment.	We have made inquiries with appropriate personnel at the data processor.	No exceptions noted.

Control area C		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
▶ The Data Processor performs background check in accordance with the Data Processors procedure and the function, which the candidate is to take.	We have inspected the data processor's on-boarding procedure for new employees. We have observed that references should be obtained if it is deemed necessary by the management or the HR department, as well as criminal records checks. On a sample basis we have inspected that the hiring procedure is followed when hiring new staff.	
Resignation of employees ▶ The Data Processor has prepared and implemented a procedure for resignation of employees the end of the employment.	We have made inquiries with appropriate personnel at the data processor. We have inspected the data processor's off-boarding procedure. On a sample basis we have inspected that the access rights of departed employees have been removed from the data processor's systems in accordance with the off-boarding procedure.	No exceptions noted.
Training and instruction of employees processing personal data. ▶ The Data Processor conducts awareness training of new employees in accordance with data protection and information security, in continuation of the employment. ▶ The Data Processor conduct's introduction courses for new employees, regarding how data controllers are to process data.	We have made inquiries with appropriate personnel at the data processor. We have inspected that employees have a template for training and education in GDPR and the Portal. On a sample basis we have inspected that new employees have completed training in GDPR and the Portal.	No exceptions noted.
Awareness and information campaigns for employees ▶ The Data Processor conducts awareness training in data protection and information security.	We have made inquiries with appropriate personnel at the data processor.	No exceptions noted.

Control area C		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
	We have inspected that controls are in place for ongoing training of employees' knowledge of information security and data protection. We have inspected that ongoing awareness training is conducted for employees' knowledge of the latest developments in GDPR compliance. We have been informed that a part of the data processor's awareness program includes that everyone must read the latest information security policy and underlying procedures. We have inspected that all employees have read the information security policy and underlying procedures.	
Confidentiality and secrecy agreement with employees ▶ All employees are subjected statutory duty of confidentiality under the provisions of the Danish Criminal Code.	We have made inquiries with appropriate personnel at the data processor. We have inspected the data processor's employment contract template and observed that the employment contract template includes requirements for confidentiality during and after employment. On a sample basis we have inspected that the employment contract template is used.	No exceptions noted.
Obligations of security of processing and impact assessments. ▶ The data processor has procedures for assistance to the data controller on breaches of personal data security and impact analysis.	We have made inquiries with appropriate personnel at the data processor. We have inspected that the data processor has a procedure for assisting the data controller in the event of a personal data security breach and conducting a risk assessment.	No exceptions noted.

Control area C		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
	We have been informed that there have been no such incidents during the reporting period. Therefore, we have not tested the procedure for implementation and effectiveness in the declaration period.	
Audit and inspection ▶ The data processor has procedures for assistance to the data controller in relation to audit and inspection.	We have made inquiries with appropriate personnel at the data processor. We have inspected that the data processor has a procedure for assisting the data controller in relation to audits and inspections. On a sample basis we have inspected that the data processor has aided the data controller in relation to audits and inspections.	No exceptions noted.
Records of processing activities ▶ The Data Processor has established a record of processing activities as Data Processor. ▶ The record is updated with significant changes continuously. ▶ The record is updated at least once a year during the annual review.	We have made inquiries with appropriate personnel at the data processor. We have inspected that the data processor has established a register of processing activities as a data processor. We have inspected that controls are in place for updating the register at least once a year. We have inspected that the register has been updated during the declaration period.	No exceptions noted.
Storage of the record ▶ The record is stored electronically on the Data Processor's system/file drive.	We have made inquiries with appropriate personnel at the data processor.	No exceptions noted.

Control area C		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
	We have inspected that the data processor electronically stores the register in the GDPR portal.	
The Danish Data Protection Agency's access to the record ▶ The Data Processor hands over the record at the request of the Danish Data Protection Agency.	We have made inquiries with appropriate personnel at the data processor. We have been informed that the data processor provides the register upon request from the Data Protection Authority. We have been informed that there are no previous examples of requests from the Data Protection Authority, which is why we have not been able to verify the control.	No exceptions noted.

Control area D		
Control Objective ▶ *To ensure that the Data Processor can delete and return personal data when the service regarding the processing has terminated, in accordance with instruction from the Controller.*		
Control activities	**Test performed by BDO**	**Result of test**
Deletion of personal data ▶ The Data Processor deletes the Controller's personal data per instruction, at termination of the main agreement.	We have made inquiries with appropriate personnel at the data processor. We have inspected the data processor's data processing template and observed that upon termination of services related to the processing of personal data, the data processor is obligated to delete all personal data that has been processed on behalf of the data controller. We have inspected the data processor's data deletion procedure and observed that those responsible for systems containing personal data are responsible for ensuring that data that is no longer necessary for the purpose of processing is deleted and in compliance with other legislation. We have observed that the procedure has been updated within the last year. On a sample basis we have inspected that data from terminated clients has been deleted after the termination of the cooperation.	No exceptions noted.

Control area E

Control Objective

- *Procedures and controls are followed, which ensure that the data processor only stores personal data in accordance with the agreement with the data controller.*

Control activities	Test performed by BDO	Result of test
Storage of personal data ▶ There are written procedures which contain requirements that the storage of personal data be only conducted in accordance with the contract with the data controller and the list of locations in the associated data processing agreement. ▶ An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have made inquiries with appropriate personnel at the data processor. We have inspected the data processor's standard data processing agreements. We have inspected the data processor's data retention procedure and observed that data may only be retained in accordance with the purposes specified in the concluded data processing agreements. We have observed that the procedure has been updated within the last year.	No exceptions noted.
Location of storage of personal data ▶ The data processor's data processing, including storage, must only take place in the locations, countries, or territories approved by the data controller.	We have made inquiries with appropriate personnel at the data processor. We have inspected the data processor's standard data processing agreements and observed that the data controller must be notified before any changes in the location of personal data storage. We have observed that the data controller must approve any changes in the use of sub-processors. We have been informed that there have been no changes in the locations for the storage of the data controller's personal data.	No exceptions noted.

Control area F

Control Objective

- *Procedures and controls are followed to ensure that only approved sub-processors are used, and that the data processor, by following up on their technical and organisational measures to protect the data subjects' rights and the processing of personal data, ensures satisfactory processing security.*

Control activities	Test performed by BDO	Result of test
Sub data processor agreement and instruction ▶ There are written procedures which contain requirements for the data processor when using sub-data processors, including requirements for sub-data processor agreements and instructions.	We have made inquiries with appropriate personnel at the data processor. We have inspected the data processor's standard data processing agreements and observed that the data processor must impose on sub-processors the same data protection obligations as the data processor itself. The data processor must also enter into data processing agreements with related instructions. We have observed that the data processor uses three sub-processors for the processing of personal data. We have inspected the concluded sub-processor agreements and observed that the data processor has imposed on the sub-processors the same data protection obligations as those to which the data processor is subject.	No exceptions noted.
Approval of sub data processors ▶ The Data Processor only use approved sub processors.	We have made inquiries with appropriate personnel at the data processor. We have inspected the data processor's standard data processing agreements and observed that the data controller specifically approves the use of sub-processors. On a sample basis we have inspected data processing agreements for the GDPR portal and the Whistleblower scheme and observed that the data processing agreements contain information about the use of sub-processors.	No exceptions noted.

Control area F		
Control Objective ▶ *Procedures and controls are followed to ensure that only approved sub-processors are used, and that the data processor, by following up on their technical and organisational measures to protect the data subjects' rights and the processing of personal data, ensures satisfactory processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
Changes to approved sub data processors ▶ In the event of changes in the use of generally approved sub-processors, the data controller is notified in a timely manner in relation to being able to object and/or withdraw personal data from the processor.	We have made inquiries with appropriate personnel at the data processor. We have inspected the data processor's standard data processing agreements and observed that the data controller must approve any changes in the use of sub-processors. We have been informed upon inquiry that there have been no changes in the use of sub-processors during the declaration period. Therefore, we have not tested the procedure for implementation and effectiveness in the declaration period.	No exceptions noted.
Overview of approved sub data processors ▶ The Data Processor has an overview of approved sub processors. Overview of approved sub processors contains among other things information about contact person, location for processing and type of processing and category of personal data, which the sub processor undertakes.	We have made inquiries with appropriate personnel at the data processor. We have inspected the data processor's standard data processing agreements. We have observed that both agreements include a list of approved sub-processors with their names, addresses, and a description of the processing.	No exceptions noted.
Supervision of sub processors ▶ The data processor supervises its sub-data processors by, among other things, obtaining auditor statements of the type ISAE 3000, SOC 2 and ISO 27001 certification or similar documentation based on a risk assessment of the data processor construction.	We have made inquiries with relevant personnel at the data processor. We have inspected that there is an annual control for monitoring sub-processors. We have inspected that the data processor has supervised its sub processors, which include the following sub processors:	No exceptions noted.

Control area F		
Control Objective ▶ *Procedures and controls are followed to ensure that only approved sub-processors are used, and that the data processor, by following up on their technical and organisational measures to protect the data subjects' rights and the processing of personal data, ensures satisfactory processing security.*		
Control activities	**Test performed by BDO**	**Result of test**
	➢ Hetzner GMBH's ISO 27001:2013 certification, valid from September 27, 2022, to September 26, 2025. In addition, we have inspected a security report on the setup and control of technical and organizational security measures at Hetzner GMBH. ➢ Flowmailer B.V's ISO 27001:2013 certification, valid from December 9, 2020, to March 13, 2024. Based on a risk assessment, no additional actions have been taken in relation to Flowmailer B.V. ➢ Physical inspection of Timbed. Based on a risk assessment, the physical inspection is accepted, and no additional actions have been taken in relation to Timbed.	

Control area H

Control Objective

- *Procedures and controls are followed, which ensure that the data processor can assist the data controller with the provision, correction, deletion, or restrictions of information on the processing of personal data to the data subject.*

Control activities	Test performed by BDO	Result of test
The data subjects' rights ▶ The Data Processor has prepared a procedure for assistance to the Controller at fulfilling the data subjects' rights. ▶ It is possible to provide insight into all information registered in (system/service).	We have queried relevant personnel at the data processor. We have inspected the data processor's procedures related to the rights of data subjects and observed that the data processor has established procedures that enable timely assistance to the data controller in relation to providing access, rectification, erasure, or restriction of and information about the processing of personal data to the data subject. We have observed that the procedure was updated within the last year. We have been informed that there have been no such incidents during the reporting period. Consequently, we have not tested the implementation and effectiveness of the procedure in the declaration period.	No exceptions noted.

Control area I		
Control Objective ▶ *Procedures and controls are followed to ensure that any security breaches can be managed in accordance with the relevant data processor agreement.*		
Control activities	**Test performed by BDO**	**Result of test**
Communication of personal data breach ▶ The Data Processor communicates to the Controller the personal data breach without undue delay. ▶ The Data Processor updates the Controller on all information relevant and necessary when the information is available to the Data Processor. ▶ Communication between Data Processor and Controller is documented and stored.	We have queried relevant personnel at the data processor. We have inspected the data processor's standard data processing agreements and observed that the data processor promptly notifies, and if possible, within 48 hours, the data controller upon becoming aware of a personal data breach. We have inspected the data processor's procedures for notifying the data controllers in case of personal data breaches and observed that the data controller must be notified as soon as possible and within 48 hours. We have observed that the procedure was updated within the last year. We have been informed that the data processor has not experienced any personal data breaches related to the GDPR portal or the Whistleblower scheme. Therefore, we have not tested the implementation and effectiveness of the procedure in the declarations period.	No exceptions noted.
Identification of personal data breaches ▶ The Data Processor performs surveillance for detecting breaches of the personal data security. ▶ The Data Processor has prepared a procedure for assessing and identifying personal data breaches.	We have queried relevant personnel at the data processor. We have inspected the data processor's controls for ongoing awareness training of employees in Information Security and GDPR. We have inspected that there is continuous awareness training for employees on GDPR compliance. We have been informed that part of the data processor's awareness program includes the requirement for all employees to	No exceptions noted.

Control area I		
Control Objective ▶ *Procedures and controls are followed to ensure that any security breaches can be managed in accordance with the relevant data processor agreement.*		
Control activities	**Test performed by BDO**	**Result of test**
	read the latest information security policy and underlying procedures, including the procedure for identifying personal data breaches. We have inspected that all employees have read the information security policy and underlying procedure.	
Registration of personal data breaches ▶ The Data Processor registers personal data breaches in the data breach log. ▶ The Data Processor has prepared and implemented a procedure for experience gathering when personal data is breached.	We have queried relevant personnel at the data processor. We have inspected the data processor's procedure for personal data breaches and observed that breaches must be recorded in the data breach log in accordance with the data processor's procedure. We have been informed that the data processor has not experienced any breaches of personal data related to the GDPR portal or the Whistleblower system. Therefore, we have not tested the procedure for implementation and effectiveness in the declarations period.	No exceptions noted.
Assisting the data controller with handling personal data breaches ▶ Procedures for assistance to the Controller when assisting in relation to articles 33-34 and 36 have been prepared.	We have queried relevant personnel at the data processor. We have inspected the data processor's standard data processing agreements and observed that the data processor is required to assist the data controller in their reporting to the Data Protection Authority. We have inspected the data processor's procedures for providing assistance to the data controller in their reporting to the Data Protection Authority.	No exceptions noted.

Control area I		
Control Objective ▶ *Procedures and controls are followed to ensure that any security breaches can be managed in accordance with the relevant data processor agreement.*		
Control activities	**Test performed by BDO**	**Result of test**
	We have been informed that there have been no incidents related to assisting the data controller in their reporting to the Data Protection Authority. Therefore, we have not tested the procedure for implementation and effectiveness in the declaration period.	

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

HAVNEHOLMEN 29
1561 KØBENHAVN V

CVR NO. 20 22 26 70

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

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

Jacob Martin Barlach
CTO
Serienummer: 63a7b013-50b5-4470-b3cd-1797a4659b34
IP: 80.208.xxx.xxx
2023-11-24 09:30:29 UTC

Mikkel Jon Larssen
BDO STATSAUTORISERET REVISIONSAKTIESELSKAB CVR: 20222670
Partner
Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff
IP: 77.243.xxx.xxx
2023-11-24 09:36:13 UTC

Claus Bonde Hansen
BDO STATSAUTORISERET REVISIONSAKTIESELSKAB CVR: 20222670
Statsautoriseret revisor
Serienummer: 92ede3e7-9e85-40a7-9d75-0bcfcab9c71a
IP: 130.227.xxx.xxx
2023-11-24 12:01:27 UTC