SAMESYSTEM A/S

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT AT 5 SEPTEMBER 2023 ON THE DESCRIPTION OF SAMESYSTEM 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 DANISH ACT ON SUPPLEMENTARY PROVISIONS

This English document is an unofficial translation of the original Danish assurance report, and in case of any discrepancy between the original Danish assurance report and the English translation, the Danish text shall prevail.

CONTENTS

1. INDEPENDENT AUDITOR'S REPORT

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT AT 5 SEPTEMBER 2023 ON THE DESCRIPTION OF SAMESYSTEM AND NAME OF THE COMPANY 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 DANISH ACT ON SUPPLEMENTARY PROVISIONS

To: The Management of Samesystem A/S
Samesystem A/S' Customers

Scope

We have been engaged to report on SameSystem A/S' (the data processor) description in section 3 of SameSystem and SameSystem A/S 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 of the technical and organisational measures and other controls related to the control objectives stated in the description 5 September 2023.

We have not performed procedures regarding the operating effectiveness of the controls stated in the description, and accordingly, we do not express an opinion on this.

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 and implementing 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 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 and design 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 of the controls. The procedures selected depend on the auditor's judgement, including the assessment of the risks that the description is not fairly presented, and that controls are not appropriately designed. 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.

As described above, we have not performed procedures regarding the operating effectiveness of the controls stated in the description and, accordingly, we do not express an opinion on this.

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 SameSystem and SameSystem A/S, that each individual Data 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.

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 SameSystem 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 5 September 2023.

b. The technical and organisational measures and other controls, relating to the control objectives stated in the description were appropriately designed 5 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 SameSystem, 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, 26 September 2023

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, State Authorised Public Accountant

Mikkel Jon Larssen
Partner, Head of Risk Assurance, CISA, CRISC

2. SAMESYSTEM A/S' STATEMENT

SameSystem A/S processes personal data in relation to SameSystem 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 SameSystem, 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.

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

SameSystem A/S confirms that the accompanying description in section 3 fairly presents SameSystem, that has processed personal data for the Data Controllers subject to the EU General Data Protection Regulation, and the related technical and organisational measures (controls) at 5 September 2023. The criteria used in making this statement were that we:

1. Presents how SameSystem, and the related technical and organisational measures and other controls were 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 SameSystem 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.

1. Does not omit or distort information relevant to the scope of SameSystem 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 SameSystem that the individual data controllers might consider important in their environment.

SameSystem 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 at 5 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.

SameSystem 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.

Copenhagen, 26 September 2023

SameSystem A/S

Carsten Fensholt
CEO

3. SAMESYSTEM A/S' DESCRIPTION OF SAMESYSTEM

SAMESYSTEM A/S

SameSystem is a company listed at NASDAQ First North and develops and runs an online workforce management solution for retail and food service which handles planning and administration.

The workforce management solution (SameSystem) focuses solely on what matters within shops, cafees and restaurants: to boost growth, reduce expenses, safe time and ensure motivated employees.

SameSystem has development and sales offices in Denmark and Lithuania as well as sales offices in Spain, Germany and Norway. SameSystem's approx. 100 employees are specialised within system development, server operation, support, sales and information security. SameSystem is organised in the following departments:

Product	Development and operation of the SameSystem platform
Customer Success	Implementation, support and key account management
Sales	Canvassing of the SameSystem platform
Administration	Bookkeeping, IT, Law, etc.

The administration department controls SameSystem's security of personal data in relation to the processing that SameSystem handles on behalf of their clients, including entering into data processing agreements, replying to inquiries from the data controller, communication of personal data breach, compliance with internal policies and procedures, etc.

SAMESYSTEM AND PROCESSING OF PERSONAL DATA

SameSystem provides the SameSystem platform as a Software-as-a-Service (SaaS) solution. The SameSystem platform consists of a web application and a relating mobile app.

The SameSystem platform is developed in Denmark and Lithuania but is controlled from hosting centres in Germany and Finland. Other subprocessors are used for storage of back-up, sending out mails and text messages, chat and digital signatures. SameSystem has entered data processing agreements with these subprocessors.

SameSystem processes personal data on behalf of their clients, who are data processors, when they apply the SameSystem platform for workforce management. SameSystem has entered data processing agreements with the data controllers on this processing.

The personal data being processed fall under article 6.1.b of the General Data Protection Regulation (Contractual agreement) on common personal data and include, among others, personal name, e-mail address, telephone number, personal identification number, bank information as well as other HR and payroll information about the data controller's employees.

MANAGEMENT OF THE SECURITY OF PERSONAL DATA

SameSystem has prepared requirements for establishing, implementing, maintaining, and improving a management system for the security of personal data, which ensure compliance with the concluded agreements with the data controllers, good data processor practice, and relevant requirements for data processors in accordance with the General Data Protection Regulation and the Danish Data Protection Act.

The technical and organisational security measures and other controls for protection of personal data are designed in accordance with the risk assessments and implemented to ensure confidentiality, integrity, and accessibility together with compliance with current data protection legislation. Security measures and controls are wherever possible automated and technically supported by IT systems.

Management of the security of personal data and the technical and organisation security measures and other controls are structured in the following key areas, for which control objectives and control activities have been defined:

ARTICLE	AREA
Article 28 (1)	The Processor's guarantees
Article 28 (3)	Data processor agreement
Article 28 (3)(a)(h) and (10) Article 29 Article 32 (4)	Instruction for processing of personal data
Article 28 (2) and (4)	Sub-processors
Article 28 (3)(b)	Confidentiality and statutory professional secrecy
Article 28 (3)(c)	Technical and organisational security measures
Article 25	Data protection by design and by default.
Article 28 (3)(g)	Deletion and return of personal data
Article 28 (3)(e)(f)(h)	Assistance to the Controller
Article 30 (2) (3) (4)	Records of processing activities
Article 33 (2)	Communication of personal data breach.
Articles 44-49	Transmission of personal data to third countries

RISK ASSESSMENT

SameSystem manages risks in its deliverables on the basis of a risk management process. Among other things, the risk management comprises:

- Identification of potential risks which may impact the individual deliverables, both from a technical and commercial view.
- Assessment of the identified potential risks, materiality, probability and consequences for the individual deliverables.
- That initiatives, for reduction of the probability of risks occurring, are implemented in a cost-effective way.

Control objectives and controls, which meet the risks, have been selected based on the General Data Protection Regulation and adjusted to the necessary extent, including with inspiration from ISO 27001. Description of control objectives appears from the the paragraph, auditor's results of test of controls.

The risk assessment includes mapping of all the known risks implied by the processing and a categorisation (scoring, probability and seriousness) of these as well as initiatives for minimisation of mapped risks. The purpose is that SameSystem lives up to high standards focusing on high confidentiality, integrity and availability.

Based on the risk assessment, an information security policy has been prepared and implemented with several procedures for specific areas.

It is considered that SameSystem deliverables do not imply a high risk when processing personal data. Should this be the case, SameSystem will go into a close dialogue with the data controller and in collaboration with the data controller carry out a data protection impact assessment.

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES AND OTHER CONTROLS

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

The data processor's guarantees

SameSystem has introduced policies and procedures ensuring that SameSystem can provide the sufficient guarantees for completing appropriate technical and organisational security measures in such a way that the processing complies with the requirements of the General Data Protection Regulation and ensures protection of the data subject's rights. SameSystem has implemented an IT security policy, which is approved by Management and will be reviewed and updated continuously. There are procedures for recruiting and resignation of employees.

Data processing agreement

SameSystem enters data processing agreements with the clients to ensure that SameSystem in relation to the client contract enters a data processing agreement stating the conditions for processing personal data on behalf of the data controller. SameSystem applies a template for data processing agreements in accordance with the service provided, including information on the use of subprocessors. The data processing agreements are digitally signed and stored electronically.

Instructions for processing personal data

SameSystem has introduced policies and procedures ensuring that SameSystem acts according to the instruction given by the data controller in the data processing agreement. The instruction is maintained with procedures instructing employees in how processing of personal data must be done, including who at the data controller may give binding instructions to SameSystem. Moreover, the procedures ensures that SameSystem informs the data controller, when their instructions are not perceived to be following data protection legislation.

Subprocessors

SameSystem assesses the subprocessor and the guarantees provided by them before an agreement is made to ensure that the subprocessor is able to observe the obligations imposed on Samesystem.

SameSystem has carried out an annual review of their subprocessors based on a risk assessment of the specific processing of personal data, by among other things, obtaining ISAE 3000 or SOC 2 assurance reports by auditor, or similar documentation, when possible.

Confidentiality and statutory professional secrecy

All employees at SameSystem have committed to confidentiality by signing an employment contract which contains terms of professional secrecy and confidentiality.

Technical and organisational security measures

Risk Assessment

SameSystem has completed the technical and organisational security measures based on an assessment of risks in relation to confidentiality, integrity, and accessibility. Please refer to specific section about this.

Contingency plans

SameSystem may in time restore the accessibility of and access to personal data in case of physical and technical incidents. SameSystem has established emergency preparedness plans taking effect in these cases. Organisation of an emergency preparedness group is established and guidelines for activation of the emergency preparedness are introduced.

Storage of personal data

SameSystem ensures that personal data are only stored in accordance with the contract with the data controller and according to the list of locations in the relating data processing agreement.

Physical access control
SameSystem has introduced procedures ensuring that rooms are protected against unauthorised access. Only persons with a work-related or other legitimate needs have access to the rooms, and special security measures have been taken for areas, where personal data is processed. Clients, suppliers, and other visitors must be escorted.

SameSystem's hosting supplier has introduced procedures ensuring that access to server rooms is allocated based on a work-related need. Service organisations, who need access to supervise or keep watch, are approved by the management. Allocated accesses to server rooms are examined and revised in connection with changes and at least once a year at the responsibility of the supplier.

Physical security
SameSystem has introduced procedures ensuring that servers are protected against unauthorised access, damage, service suspensions and similar by means of special security measures.

Thus, servers are kept with external hosting partners in specially designed server rooms with physical and electronic access control and logging of access. The server room is protected from environmental threats such as fire, water infiltration, damp, overheating, power failure and overload. Systems for environmental protection of operating facilities are serviced and maintained on a current basis according to the directions of the service organisations, respectively. The operating environment is monitored by SameSystem.

Logical access security
SameSystem has introduced procedures ensuring that access to systems and data are protected by an authorisation system. User is set up with unique user identification and password, and user identification is used in connection with allocation of resources and systems. All allocation of rights in systems is based on a work-related need.

The design of rules for i.a. length, complexity, regular changes to and history of password and termination of user account after unsuccessful log-on attempts follows best practice for a secure logical access control. Technical measures have been established to support these rules.

Technical measures have been designed to ensure that all SameSystem’s employees’ access to personal data on the SameSystem platform are protected with two-factor authentication no matter from where the system is accessed.

Remote workstations and remote access to systems and data
SameSystem has introduced procedures to ensure that access to back-end systems and development environments outside of SameSystem's premises as well as remote access to systems and data take place via VPN connections and two-factor authentication.

External communication lines
SameSystem has introduced procedures to ensure that external communication line are secured with strong encryption and that email and other communication containing sensitive personal information are encrypted in the transmission using TLS.

Encryption of personal data
SameSystem has introduced procedures ensuring that databases containing personal data are encrypted and that the same goes for backup copies. Recovery keys and certificates are stored properly.

SameSystem has introduced procedures to ensure that data on personal devices are encrypted at the commencement of use so that data can only be accessed by authorised users. Recovery keys and certificates are stored properly.

Firewall
SameSystem has introduced technical measures to ensure that traffic between the internet and the network is controlled by a firewall. External access by means of ports in the firewall is limited wherever possible, and access rights are allocated through actual ports for specific segments. Workstations uses firewall.

Antivirus programme
SameSystem has introduced antivirus to ensure that devices with access to networks and applications are protected against virus and malware. Antivirus programmes and other protection systems are currently updated and adjusted.

Vulnerability scanning and penetration testing
SameSystem has introduced procedures to ensure that systems have been introduced to identify and respond to technical vulnerabilities in applications, services and infra structure, so that loss of confidentiality, integrity and accessibility of systems and data can be avoided.

Back-up and re-establishing of data
SameSystem has introduced backup to ensure that systems and data are synchronised to redundant and geographically separated environment in Germany and Finland and that all data are backed up to meet loss of data or loss of accessibility at crashes.
Backups are stored in an alternative cloud location and are protected with both physical and logical security measures, which prevent data from falling into the hands of unauthorised persons or that back-ups are destroyed by fire, water, malicious damage, or accidental damage.

Maintenance of system software
SameSystem's systems are operated in a Docker Cloud environment. When you deploy in a Docker Cloud environment you automatically get the most recent versions of the system environment each time. Therefore, there is no formal process or procedure for maintenance of system software, as it takes place automatically.

Logging in systems, databases, and network
SameSystem has introduced VPN and logging, which have been set up according to 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 demonstrate possible unauthorised use of systems or data. Log data is secured against loss and erasure.
External access to databases must be approved by 4 people. Actions in the database are logged.

Monitoring
SameSystem has introduced monitoring of the resources and errors of the system. This is managed reactively in Kibana to ensure that systems and the technical security measures introduced are monitored on a continuous basis.

Repair and service as well as disposal of IT equipment
SameSystem does not release storage media for destruction. Hard disks are encrypted at repair and are not accessible without the user’s password.
All computers are set up with encryption of storage media and Microsoft Endpoint Manager.
Login to computers is via two-factor authentication.

Testing, assessment and evaluation
SameSystem has introduced procedures for regular testing, assessment, and evaluation of the efficiency of the technical and organisational security measures to secure the processing security through implementation of an annual wheel and governance tool.

Data protection through design and standard settings

SameSystem has introduced policies and procedures for development and maintenance of the SameSystem platform to ensure a controlled change process. A Change Management system is applied to manage development and change tasks, and all tasks follow a uniform process.

Development and production environments are separated. Any development task goes through a testing cycle and anonymised personal data in a development environment. Procedures are introduced for version control, logging, and back-up so that it is possible to re-install previous versions.

Deletion and return of personal data

SameSystem has introduced policies and procedures to ensure that personal data are deleted or returned in accordance with instruction from the Controller, when the processing of personal data terminates at the end of contract with the Controller.

Assistance to the data controller

SameSystem has introduced policies and procedures to ensure that SameSystem can assist the data controller in complying with their obligation to reply to requests on executing the data subjects' rights.

SameSystem has introduced policies and procedures to ensure that SameSystem can assist the data controller in ensuring compliance with the obligations of article 32 on security of processing, article 33 on notification and communication of personal data breach, and article 34 - 36 on data protection impact assessment.

SameSystem has introduced policies and procedures ensuring that SameSystem is able to provide to the data controller all information necessary to demonstrate compliance with the requirements for data processors. Besides, SameSystem allows and assists in audits, including inspections performed by the Controller or others, who are authorised to do this by the Controller.

Record of categories of processing activities

SameSystem has introduced policies and procedures ensuring that a record is kept of categories of processing activities performed on behalf of the data controller. The record is updated regularly and controlled during the annual examination of policies and procedures, etc. The record is stored electronically and may be made available for the supervisory authority, upon request.

Communication of personal data breach

SameSystem has introduced policies and procedures ensuring that personal data breaches are registered with detailed information about the incident and that the data controller receives communication without undue delay after SameSystem has become aware of the personal data breach. The registered information makes the data controller able to assess whether the personal data breach must be notified to the supervisory authority and whether the personal data breach must be communicated to the data subjects.

Transmission of personal data to third countries

SameSystem has introduced policies and procedures to ensure that the transfer of personal data to sub-processors in non-EU countries takes place in accordance with the SCC (standard contract) of the General Data Protection Regulation or other valid transfer basis and as instructed by the data controller. It is SameSystem's endeavour that suppliers and data are placed within the borders of EU.

COMPLEMENTARY CONTROLS WITH THE CONTROLLER

The Controller is obligated to implement the following technical and organisational security measures and other controls to reach the control objectives and thereby comply with the data protection legislation:

- The data controller must ensure that the instruction from the data controller is always legal according to the data protection legislation applicable and that the instruction is appropriate compared to the entered contract and the data processing agreement.

- The data controller is responsible for ensuring that the administrators' use of the SameSystem platform and the processing of personal data conducted in the system are in accordance with the data protection legislation.
- The data controller manages the user privileges in the SameSystem platform, including who are allocated administrator access and which rights the individual administrators are allocated.
- The data controller is advised against to use the platforms for processing, including storage of sensitive personal data, and it is the data controller's responsibility to ensure that such data are not part of or uploaded to the platforms.

4. CONTROL OBJECTIVES, CONTROLS, TESTS AND RESULTS OF TESTS

Purpose and scope

BDO has performed their work in accordance with ISAE 3000 on other assurance engagements with certainty than audit or review of historical financial information.

BDO has performed procedures to obtain evidence of the information in SameSystem A/S' description of SameSystem and for the design of the relating technical and organisational security measures and other controls. The actions selected depend on BDO's assessment, including the assessment of the risks of the description not being fair and that the controls are not appropriately designed.

BDO's test of the design of the technical and organisational security measures and other controls as well as the implementation hereof have included the control objectives and the relating control activities selected by SameSystem A/S and which are apparent in the subsequent control form.

In the control form, BDO has described the tests performed, which were assessed as necessary in order to obtain a reasonable degree of assurance that the stated control objectives were achieved, and the related controls were appropriately designed and implemented at 05 September 2023.

Performed test procedures

Test of the design of the technical and organisational security measures and other controls as well as the implementation hereof is performed by inquiry, inspection, and observation.

Type	Description
Inquiries	Interviews of relevant personnel have been performed for all significant control activities. The purpose of the interviews was among other things 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 containing information about the performance of the control, have been read for the purpose of assessing the design and monitoring of the specific controls, and whether the controls are designed so that they can be 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 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 is implemented.

For the services provided by Hetzner Online GmbH for hosting in the period, we have received a ISO 27001 certification applicable until 26 September 2025 and a SoA report at 30 May 2022 for the subprocessors' technical and organisational security measures and other controls.

For the services provided by Scaleway SAS within backup, we have received a ISO 27001 certification applicable until 14 February 2024 for the subprocessor's technical and organisational security measures and other controls.

For the services provided by Link Mobility Group within delivery of text messages, we have received an ISAE 3000 assurance report at 15 March 2023 of the subprocessor's technical and organisational security measures and other controls.

For the services provided by SMTP.DK ApS within delivery of text messages, we have received the data processor's performed inspection in the form of an filled questionnaire as at 16 August 2023 for the sub-processor's technical and organisational security measures and other controls.

For the services provided by E-Signatur Danmark A/S within digital signatures, we have received an ISAE 3000 assurance report at 30 June 2022 of the subprocessor's technical and organisational security measures and other controls.

For the services provided by Sendbird, Inc. within chat and communication services, we have received an ISO 27001 certification applicable until 24 July 2024 for the subprocessor's technical and organisational security measures and other controls.

These subprocessors' relevant control objectives and related controls are not included in SameSystem's description of SameSystem and the relating technical and organisational security measures and other controls. Thus, we have only inspected the received documentation and tested the controls with SameSystem A/S, which ensure the performance of a duly supervision of the subprocessor's compliance with the data processing agreement entered between the subprocessor and the data processor as well as compliance with the General Data Protection Regulation and the Data Protection Act.

Result of test

The result of the tests of technical and organisational security measures and other controls shows whether the tests described has given rise to note exceptions.

An exception exists when:

- Technical or organisational security measures or other controls are to be designed and implemented to fulfil a control objective.
- Technical or organisational security measures or other controls related to a control objective are not suitably designed or implemented.

Article 28 (1) The data processor's guarantees

Control objectives

- *To ensure that the data processor is able to provide the sufficient guarantees for protection of the data controller's personal data in accordance with the requirements of the General Data Protection Regulation and the protection of the data subject's rights.*

Control objectives	Test performed by BDO	Result of test
Information Security Policy ▶ The Processor has prepared and implemented an information security policy.	We have interviewed relevant personnel with the Processor. We have inspected the data processor's information security policy and observed that it is implemented. We have inspected that the data processor's employees have been trained in the information security policy.	No exceptions noted.
Review of the information security policy ▶ The Processor's information security policy is reviewed and updated at least once annually.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's annual wheel, of which it appears that the information security policy is reviewed and updated at least once a year.	No exceptions noted.
Organisation of Information Security ▶ The data processor has documented and established management control of information security.	We have interviewed relevant personnel with the Processor. We have inspected the data processor's information security policy and observed that those charged with governance have the overall responsibility for the information security policy. We have inspected the data processor's annual wheel and observed that the data processor has established management control of the information security.	No exceptions noted.

Article 28 (1) The data processor's guarantees

Control objectives

- *To ensure that the data processor is able to provide the sufficient guarantees for protection of the data controller's personal data in accordance with the requirements of the General Data Protection Regulation and the protection of the data subject's rights.*

Control objectives	Test performed by BDO	Result of test
Recruitment of employees ▶ The data processor performs screening of potential employees before employment.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's procedure for recruiting employees, of which it is evident that the data processor performs screening of potential employees prior to employment. For the most recent hired employee, we have inspected that the procedure has been followed.	No exceptions noted.
Resignation of employees ▶ The data processor has developed and implemented a procedure for off-boarding of resigned employees.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's procedure for resignation of employees. For the most recent resigned employee, we have inspected that the procedure has been followed.	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. ▶ Introduction courses are conducted for new employees, including about the processing of data controllers' personal data.	We have interviewed relevant personnel with the Processor. We have inspected documentation of the data processor's conduct of awareness training for employees about data protection and information security. We have inspected documentation for that the data processor has conducted a introduction course about the processing of data controllers' personal data for new employees.	No exceptions noted.

Article 28 (1) The data processor's guarantees		
Control objectives ▶ *To ensure that the data processor is able to provide the sufficient guarantees for protection of the data controller's personal data in accordance with the requirements of the General Data Protection Regulation and the protection of the data subject's rights.*		
Control objectives	**Test performed by BDO**	**Result of test**
▶ The data processor conducts training of employees on an ongoing basis in accordance with data protection and information security and handling hereof.	We have inspected the data processor's annual wheel and observed that the data processor currently conducts training of employees in accordance with data protection and information security and handling hereof. We have inspected documentation for that the data processor conducts training of employees on an ongoing basis in accordance with data protection and information security and handling hereof.	
Awareness and information campaigns for employees. ▶ The data processor conducts awareness training on an ongoing basis in the form of morning meetings, notices, etc. ▶ The data processor conducts information campaigns for employees on data protection and information security.	We have interviewed relevant personnel with the data processor. We have inspected documentation of awareness campaigns being conducted on an ongoing basis by the data processor. We have inspected documentation of awareness campaigns on data protection and information security being conducted on an ongoing basis by the data processor.	No exceptions noted.

Article 28 (3): Data processing agreement		
Control objectives ▶ *To ensure that the data processor enters a written contract with the data controller, which determines the terms for the processing of the data controller's personal data and that the contract is stored electronically.*		
Control activity	**Test performed by BDO**	**Result of test**
Entering into a data processor agreement with the Controller ▶ The data processor applies a data processing agreement template for entering into data processing agreements. ▶ Applicable data processing agreements are stored electronically. ▶ Data processing agreements contain information about the use of subprocessors.	We have interviewed relevant personnel with the Processor. We have inspected the data processor's template for data processing agreements and the entered data processing agreements. We have inspected documentation of that data processing agreements are stored electronically. We have inspected the data processor's data processing agreements and observed that they contain information about the use of subprocessors.	No exceptions noted.

Article 28 (3) and (10), article 29, and article 32 (4): Instructions for processing personal data		
Control objectives ▶ *To ensure that the data processor solely acts according to documented instructions from the data controller.* ▶ *To ensure that the data processor notifies the data controller, if an instruction is in contravention of the General Data Protection Regulation and the Data Protection Act.*		
Control objectives	**Test performed by BDO**	**Result of test**
Instructions for processing personal data ▶ Entered data processing agreement contains instructions from the data controller. ▶ The data processor obtains instruction for processing personal data from the data controller in connection with entering into a data processing agreement.	We have interviewed relevant personnel with the Processor. We have inspected entered data processing agreements and observed that they contain instructions from the data controller.	No exceptions noted.
Compliance with instruction for processing of personal data ▶ The data processor solely processes personal data as per instruction from the data controller. ▶ The data processor performs self-control of compliance with the instructions of entered data processing agreements.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's record of processing activities as data processor, and we observed that the processing is in accordance with instructions from data controllers. We have inspected the data processor's annual wheel and observed that the data processor has performed self-control of compliance with instructions of entered data processing agreements.	No exceptions noted.
Communication of unlawful instruction to the data controller ▶ The data processor communicates immediately to the data controller, if the data controller's instruction is in contravention of the data protection legislation.	We have interviewed relevant personnel with the data processor. By inquiry, we have been informed that there were no cases of instructions assessed to be in contravention of the data protection legislation, for which reason we were not able to test the control introduced.	No exceptions noted.

Article 28 (2) and (4): Subprocessors

Control objectives

- *To ensure that the subprocessor is assigned the same data protection obligations as the data processor is assigned by the data controller, when entering a written contract with relating instructions.*
- *To ensure that the data controller has provided a preceding specific or general written approval of subprocessors.*
- *To ensure that the subprocessor can provide the sufficient guarantees for protection of personal data in accordance with the contract.*

Control activity	Test performed by BDO	Result of test
Subprocessor agreement and instruction ▶ When using subprocessors the data processor enters into a subprocessor agreement, which assigns the same data protection obligations to the subprocessor as the data processor is assigned. ▶ Instructions from the data controller is disclosed to the subprocessor. ▶ The data processing agreements with subprocessor are stored electronically. ▶ The data processor agreement with the subprocessor contains information about the use of subprocessors.	We have interviewed relevant personnel with the Processor. We have inspected the data processor's entered data processing agreements with subprocessors and observed that the subprocessors are imposed the same obligations as those imposed on the data processor. We have inspected the data processor's entered data processing agreements with subprocessors and observed that the data controller's instructions for the data processor have been forwarded to the subprocessor. We have inspected that data processing agreements with subprocessors are stored electronically. We have inspected the data processor's concluded data processing agreements with subprocessors and observed that the data processing agreements contain information about the use of subprocessors.	No exceptions noted.
Approval of subprocessors ▶ The Processor only applies approved subprocessors.	We have interviewed relevant personnel with the Processor. We have inspected that the data processor has entered into agreements with all subprocessors. We have observed that concluded data processing agreements contain information about the use of approved subprocessors.	No exceptions noted.

Article 28 (2) and (4): Subprocessors

Control objectives

- *To ensure that the subprocessor is assigned the same data protection obligations as the data processor is assigned by the data controller, when entering a written contract with relating instructions.*
- *To ensure that the data controller has provided a preceding specific or general written approval of subprocessors.*
- *To ensure that the subprocessor can provide the sufficient guarantees for protection of personal data in accordance with the contract.*

Control activity	Test performed by BDO	Result of test
Changes to approved subprocessors ▶ The Processor has prepared an appropriate process with the Controller for change of approved subprocessors. ▶ The Processor communicates to the Controller when changing subprocessors in connection with general approval of subprocessor. ▶ The Controller may object to changing subprocessor.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's procedure regarding change of approved subprocessors and observed that it deals with process for notification of data controllers and the opportunity for data controllers to object within a time limit of 60 days. We have inspected that the data processor in one case has started using a new subprocessor before the time limit for the data controller's opportunity to object had expired. This has entailed that data controllers' personal data have been transferred to subprocessor without the data controller's consent. By inquiry, we have been informed that the transfer was made for the purpose of testing and that the personal data were encrypted. We have inspected that the transferred personal data were encrypted.	We have ascertained that the data processor in one case has started using a new subprocessor before the time limit for the data controller's opportunity to object had expired. The subprocessor was put into service on 1 July 2023 and the deadline for objection was on 30 August 2023. No further exceptions noted.
Overview of approved subprocessors ▶ The Processor has an overview of approved subprocessors. Overview of approved subprocessors contains among other things information about contact person, location for processing and type of processing and category of personal data, which the sub data processor undertakes.	We have interviewed relevant personnel with the data processor. We have inspected that the data processor has an overview of approved subprocessors and observed that it includes all relevant information.	No exceptions noted.

Article 28 (2) and (4): Subprocessors

Control objectives

- *To ensure that the subprocessor is assigned the same data protection obligations as the data processor is assigned by the data controller, when entering a written contract with relating instructions.*
- *To ensure that the data controller has provided a preceding specific or general written approval of subprocessors.*
- *To ensure that the subprocessor can provide the sufficient guarantees for protection of personal data in accordance with the contract.*

Control activity	Test performed by BDO	Result of test
Supervision of subprocessors ▶ The Processor exercises supervision, including obtains and reviews the subprocessor's audit opinions, certifications, etc. ▶ The Processor exercises supervision of the subprocessor based on a risk assessment. ▶ The data processor exercises supervision of the subprocessor at least once annually, based on a risk assessment.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's annual wheel and observed that the data processor performs supervision of the subprocessors annually. We have inspected documentation of that the data processor has obtained and examined the subprocessor Hetzner Online GmbH's ISO 27001 certification applicable until 26 September 2025 and a SoA report at 30 May 2022 and observed that the subprocessor has responded to the material based on a risk assessment. We have inspected documentation of that the data processor has obtained and examined the subprocessor Scaleway SAS's ISO 27001 certification applicable until 14 February 2024 and observed that the subprocessor has responded to the material based on a risk assessment. We have inspected documentation of that the data processor has obtained and examined the subprocessor Link Mobility's ISAE 3000 assurance report at 15 March 2022 and observed that the subprocessor has responded to the material based on a risk assessment. We have inspected documentation of that the data processor has obtained and examined the subprocessor SMTP.DK ApS' filled out questionnaire at 16 August 2023 and observed that the subprocessor has responded to the material based on a risk assessment. We have inspected documentation of that the data processor has obtained and examined the subprocessor E-Signatur A/S' ISAE 3000 assurance report at 30 June 2022 and observed that	No exceptions noted.

Article 28 (2) and (4): Subprocessors

Control objectives

- *To ensure that the subprocessor is assigned the same data protection obligations as the data processor is assigned by the data controller, when entering a written contract with relating instructions.*
- *To ensure that the data controller has provided a preceding specific or general written approval of subprocessors.*
- *To ensure that the subprocessor can provide the sufficient guarantees for protection of personal data in accordance with the contract.*

Control activity	Test performed by BDO	Result of test
	the subprocessor has responded to the material based on a risk assessment. We have inspected documentation of that the data processor has obtained and examined the subprocessor Sendbird, Inc.'s ISO 27001 certification applicable until 24 July 2024 and observed that the subprocessor has responded to the material based on a risk assessment.	

Article 28 (3)(b): Confidentiality and statutory professional secrecy		
Control objectives ▶ *To ensure that the staff authorised to process personal data have accepted an obligation of confidentiality or are subject to an appropriate statutory professional secrecy.*		
Control activity	**Test performed by BDO**	**Result of test**
Statutory confidentiality and professional secrecy ▶ All employees are subject to statutory duty of confidentiality under the provisions of the Danish Criminal Code.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's procedures for employments and observed that the employees sign a contract of employment containing requirements for confidentiality and professional secrecy. For the most recent employee, we have inspected that the employee has signed agreement on confidentiality and professional secrecy in the contract of employment.	No exceptions noted.
Confidentiality and secrecy agreement with employees ▶ All employees have signed an employment contract, which contains a section regarding confidentiality and professional secrecy. ▶ External suppliers/consultants are subject to confidentiality and professional secrecy when entering a contract.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's procedures for employments and observed that the employees sign a contract of employment containing requirements for confidentiality and professional secrecy. For the most recent employment, we have inspected that the employee has signed agreement on confidentiality and professional secrecy in the contract of employment. By inquiry, we have been informed that no external consultants have access to personal data, for which reason we have not been able to test the control.	No exceptions noted.

Article 28 (3)(c): Technical and organisational security measures

Control objectives

- *To ensure that the data processor has implemented appropriate technical and organisational security measures taking into account the actual technical level, implementation costs and the nature, scope, coherence, and purpose of the processing concerned as well as the risks of varying probability and gravity for natural persons rights and freedoms (risk assessment), including continuous examination and update of risk assessments and security measures.*
- *To ensure that the risk assessment takes into consideration risks of accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.*
- *To ensure confidentiality, integrity, and accessibility and robustness of processing systems and services.*
- *To ensure timely restoration of the accessibility of and access to personal data in case of a physical and technical incident.*
- *To ensure procedures for regular testing, assessment, and evaluation of the efficiency of the technical and organisational security measures to ensure the processing security.*

Control activity	Test performed by BDO	Result of test
Risk assessment ▶ A risk assessment of SameSystem is carried out on an ongoing basis and at least once a year based on potential risks to the availability, confidentiality, and integrity of data in relation to the data subject's rights and freedoms. ▶ The vulnerability of systems and processes is assessed based on identified threats. ▶ Risks are minimised based on the assessment of their probability, consequence, and derived implementation costs. ▶ Risk assessments are updated on an ongoing basis when needed, but at least once a year.	We have interviewed relevant personnel with the Processor. We have inspected the data processor's risk assessment of SameSystem and observed that it is based on potential risks for the accessibility, confidentiality and integrity of data in relation to the data subject's rights and freedoms. We have observed that the vulnerability of systems and processes is assessed based on identified threats. We have inspected that the data processor has implemented compensating actions based on the probability and consequence of the risk. We have inspected the data processor's annual cycle and observed that the data processor performs review of the risk assessment. We have inspected documentation of that the data processor has performed the annual review and update of the risk assessment, and we observed that it was last updated on 8 March 2023 and that the risk assessment has been continuously updated during 2023.	No exceptions noted.
Contingency plans in case of physical or technical incidents ▶ The 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.	We have interviewed relevant personnel with the Processor. We have inspected that the data processor has established a contingency plan for the purpose of ensuring a quick response	No exceptions noted.

Article 28 (3)(c): Technical and organisational security measures

Control objectives

- *To ensure that the data processor has implemented appropriate technical and organisational security measures taking into account the actual technical level, implementation costs and the nature, scope, coherence, and purpose of the processing concerned as well as the risks of varying probability and gravity for natural persons rights and freedoms (risk assessment), including continuous examination and update of risk assessments and security measures.*
- *To ensure that the risk assessment takes into consideration risks of accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.*
- *To ensure confidentiality, integrity, and accessibility and robustness of processing systems and services.*
- *To ensure timely restoration of the accessibility of and access to personal data in case of a physical and technical incident.*
- *To ensure procedures for regular testing, assessment, and evaluation of the efficiency of the technical and organisational security measures to ensure the processing security.*

Control activity	Test performed by BDO	Result of test
▶ The data processor has established periodic testing of the contingency plan to ensure that the contingency plans are up-to-date and effective in critical situations. ▶ Tests of the contingency plans are documented and evaluated.	time to restore the accessibility of and access to personal data in a timely manner, in case of a physical or technical incident. We have inspected the data processor's annual wheel and observed that the data processor has established periodic testing of the contingency plan to ensure that the contingency plans are up-to-date and effective in critical situations.	
Storage of personal data ▶ Personal data are stored inaccessible to others. ▶ Access to personal data is granted based on work-related needs/need-to-know principles. ▶ The confidentiality of digital personal data are stored encrypted in backup and when data are transferred. ▶ Personal data are only stored as long as it is warranted/there is a legitimate reason.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's procedure for how personal data must be stored inaccessibly to others and we have observed that the procedure has been implemented. We have inspected that the data processor grants access to personal data based on work-related needs/need-to-know principles. We have inspected the data processor's annual wheel and observed that the data processor currently performs control of users with access to personal data. For employees with access to personal data, we have observed that they have a work-related need. We have inspected data in backup and transit, and we observed that these data are encrypted.	No exceptions noted.

Article 28 (3)(c): Technical and organisational security measures

Control objectives

- *To ensure that the data processor has implemented appropriate technical and organisational security measures taking into account the actual technical level, implementation costs and the nature, scope, coherence, and purpose of the processing concerned as well as the risks of varying probability and gravity for natural persons rights and freedoms (risk assessment), including continuous examination and update of risk assessments and security measures.*
- *To ensure that the risk assessment takes into consideration risks of accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.*
- *To ensure confidentiality, integrity, and accessibility and robustness of processing systems and services.*
- *To ensure timely restoration of the accessibility of and access to personal data in case of a physical and technical incident.*
- *To ensure procedures for regular testing, assessment, and evaluation of the efficiency of the technical and organisational security measures to ensure the processing security.*

Control activity	Test performed by BDO	Result of test
	We have inspected the data processor's procedure for only storing personal data as long as it is warranted/there is a legitimate reason, and we observed that the procedure has been implemented.	
Physical access control - Physical access controls have been established, which prevent the likelihood of unauthorised access to the data processor's offices, facilities, and personal data, including ensuring that only authorised persons have access. - All accesses are registered and logged. - The physical access to the data processor's offices and facilities is reviewed on an ongoing basis and at least once a year.	We have interviewed relevant personnel with the data processor. We have observed that access to the data processor's office is protected with access card to the actual building. We have inspected the the data processor's access log and observed that entries via the main entrance are logged. We have inspected the data processor's annual wheel and observed that the data processor currently reviews the access log.	No exceptions noted.
Physical security - Physical perimeter security has been established to protect areas that contain personal information. The physical perimeter security is in accordance with the adopted safety requirements. - The data processor has established controls for protection against external and environmental threats, including compliance with specified requirements for server rooms. - Building	We have interviewed relevant personnel with the data processor. We have observed that the physical security of servers at 5 September 2023 has been with the subprocessors Hetzner Online GmbH and Scaleway SAS. We have inspected documentation of that the data processor has obtained and examined the subprocessor Hetzner Online	No exceptions noted.

Article 28 (3)(c): Technical and organisational security measures

Control objectives

- *To ensure that the data processor has implemented appropriate technical and organisational security measures taking into account the actual technical level, implementation costs and the nature, scope, coherence, and purpose of the processing concerned as well as the risks of varying probability and gravity for natural persons rights and freedoms (risk assessment), including continuous examination and update of risk assessments and security measures.*
- *To ensure that the risk assessment takes into consideration risks of accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.*
- *To ensure confidentiality, integrity, and accessibility and robustness of processing systems and services.*
- *To ensure timely restoration of the accessibility of and access to personal data in case of a physical and technical incident.*
- *To ensure procedures for regular testing, assessment, and evaluation of the efficiency of the technical and organisational security measures to ensure the processing security.*

Control activity	Test performed by BDO	Result of test
○ Floors ○ Climate ○ Power ○ Access ○ Monitoring of alarm ○ Fire extinction ○ Wiring	GmbH's ISO 27001 certification applicable until 26 September 2025 and a SoA report at 30 May 2022 and observed that any deviations regarding the physical security have not been ascertained. We have inspected documentation of that the data processor has obtained and examined the subprocessor Scaleway SAS' ISO 27001 certification applicable until 14 February 2024 and through that concluded that Scaleway SAS has appropriate physical control measures.	
Logical access control ▶ The data processor has implemented a user administration procedure to ensure that user creations and closures follow a controlled process and that all user creations are authorised. ▶ User rights are assigned based on work-related needs. ▶ Privileged (administrative) access rights are granted to systems and devices based on work-related needs. ▶ Users and user rights are reviewed biannually. ▶ All accesses to systems and data are logged. ▶ The data processor has established logical access control to systems with personal data, including two-factor authorisation. ▶ The data processor has established rules for requirements for passwords which must be followed by all employees and external consultants.	We have interviewed relevant personnel with the Processor. We have inspected the data processor's procedure for user administration for the purpose of ensuring that user creations and discontinuations follow a controlled process and that all user creations are authorised, and we observed that these have been implemented. We have inspected that the data processor grants access to personal data and privileged rights based on work-related needs/need-to-know principles. For employees with access to personal data, we have observed that they have work-related needs.	No exceptions noted.

Article 28 (3)(c): Technical and organisational security measures

Control objectives

- *To ensure that the data processor has implemented appropriate technical and organisational security measures taking into account the actual technical level, implementation costs and the nature, scope, coherence, and purpose of the processing concerned as well as the risks of varying probability and gravity for natural persons rights and freedoms (risk assessment), including continuous examination and update of risk assessments and security measures.*
- *To ensure that the risk assessment takes into consideration risks of accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.*
- *To ensure confidentiality, integrity, and accessibility and robustness of processing systems and services.*
- *To ensure timely restoration of the accessibility of and access to personal data in case of a physical and technical incident.*
- *To ensure procedures for regular testing, assessment, and evaluation of the efficiency of the technical and organisational security measures to ensure the processing security.*

Control activity	Test performed by BDO	Result of test
	We have inspected the data processor's annual wheel and observed that the data processor biannually performs control of users with access to personal data. We have inspected that the data processor logs all user accesses to systems and data. We have inspected that the data processor has established logical access control for systems with personal data, and we observed that two-factor authentication is applied and that the data processor has established rules for requirements for passwords.	
Remote workplaces and remote access to systems and data - Remote access to the data processor's systems and data is via an encrypted VPN connection. - Remote access must be effected through two-factor authentication.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's network topology and actual set-up, and we observed that remote access to the data processor’s systems and data is effected through encrypted VPN connection. We have inspected that two-factor authentication must be applied at remote access.	No exceptions noted.

Article 28 (3)(c): Technical and organisational security measures

Control objectives

- *To ensure that the data processor has implemented appropriate technical and organisational security measures taking into account the actual technical level, implementation costs and the nature, scope, coherence, and purpose of the processing concerned as well as the risks of varying probability and gravity for natural persons rights and freedoms (risk assessment), including continuous examination and update of risk assessments and security measures.*
- *To ensure that the risk assessment takes into consideration risks of accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.*
- *To ensure confidentiality, integrity, and accessibility and robustness of processing systems and services.*
- *To ensure timely restoration of the accessibility of and access to personal data in case of a physical and technical incident.*
- *To ensure procedures for regular testing, assessment, and evaluation of the efficiency of the technical and organisational security measures to ensure the processing security.*

Control activity	Test performed by BDO	Result of test
External communication connections ▶ External access to systems and databases, which are used to process personal data, is done through firewall and VPN. ▶ Exchange of personal data through e-mail is done by secure e-mail (SikkerMail). ▶ External communication connections are encrypted. ▶ The data processor has an overview of which external communication connections are approved to access their network.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's network topology and actual set-up, and we observed that external access to systems and databases is effected through secure firewall and VPN. We have inspected the data processor's SMTP set-up and observed that it supports TLS 1.2 and that the data processor applies the standard settings of Microsoft Exchanges.	No exceptions noted.
Encryption of personal data ▶ The data processor has implemented an encryption policy for encryption of personal data. The policy defines the strength and protocol for encryption. ▶ Portable media with personal data are encrypted. ▶ When transmitting confidential and sensitive personal data via the internet and e-mail encryption is applied.	We have interviewed relevant personnel with the Processor. We have inspected the data processor's encryption policy for encryption of personal data and observed that it has been implemented via the data processor’s information security policy. We have observed that the policy defines how data must be encrypted and which protocols are accepted and that it has been implemented. We have inspected the data processor's encryption set-up on portable media, and we observed that these data are encrypted. We have inspected data in transit and observed that these data are encrypted.	No exceptions noted.

Article 28 (3)(c): Technical and organisational security measures

Control objectives

- *To ensure that the data processor has implemented appropriate technical and organisational security measures taking into account the actual technical level, implementation costs and the nature, scope, coherence, and purpose of the processing concerned as well as the risks of varying probability and gravity for natural persons rights and freedoms (risk assessment), including continuous examination and update of risk assessments and security measures.*
- *To ensure that the risk assessment takes into consideration risks of accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.*
- *To ensure confidentiality, integrity, and accessibility and robustness of processing systems and services.*
- *To ensure timely restoration of the accessibility of and access to personal data in case of a physical and technical incident.*
- *To ensure procedures for regular testing, assessment, and evaluation of the efficiency of the technical and organisational security measures to ensure the processing security.*

Control activity	Test performed by BDO	Result of test
Firewall ▶ The data processor has configured firewall according to best practise. ▶ The data processor only uses services/ports which are needed. ▶ Firewalls are configured and validated periodically when needed, thus, service/ports only are open when needed.	We have interviewed relevant personnel with the Processor. We have inspected the data processor's network topology and the actual set-up of firewall, and we observed that the firewall is configured according to best practice standard and that only needed services/ports are opened. We have inspected that the data processor has ensured that firewalls are configured and validated periodically when needed, thus, service/ports only are open when needed.	No exceptions noted.
Network security ▶ The network topology is structured according to best-practice principles, which means that servers which run applications cannot be accessed directly from the Internet. ▶ The data processor's network is segmented so that internal services/servers cannot communicate directly with the internet. ▶ The data processor uses known network technologies and mechanisms (Firewall/Intrusion Detection System/Intrusion Prevention System) to protect internal network.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's network topology and actual set-up, and we observed that accesses are via firewall and VPN connection and can thereby not be reached directly via the internet. We have inspected the data processor's network topology and actual set-up, and we observed that the levels have been segmented.	No exceptions noted.

Article 28 (3)(c): Technical and organisational security measures

Control objectives

- *To ensure that the data processor has implemented appropriate technical and organisational security measures taking into account the actual technical level, implementation costs and the nature, scope, coherence, and purpose of the processing concerned as well as the risks of varying probability and gravity for natural persons rights and freedoms (risk assessment), including continuous examination and update of risk assessments and security measures.*
- *To ensure that the risk assessment takes into consideration risks of accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.*
- *To ensure confidentiality, integrity, and accessibility and robustness of processing systems and services.*
- *To ensure timely restoration of the accessibility of and access to personal data in case of a physical and technical incident.*
- *To ensure procedures for regular testing, assessment, and evaluation of the efficiency of the technical and organisational security measures to ensure the processing security.*

Control activity	Test performed by BDO	Result of test
Anti-virus program ▶ Anti-virus software is installed on all workstations. ▶ Anti-virus software is updated on an ongoing basis and updated with the latest version.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's general anti-virus policy which has been activated on all workstations, and we observed that these may not be deselected. We observed that the policy ensures that antivirus is activated on all workstations and are updated currently. We have inspected one selected workstation and observed that antivirus is installed and observed.	No exceptions noted.
Penetration testing ▶ Penetration testing is performed once a year by external supplier of the data processor's network. The data processor reviews the report and follows up on ascertained weaknesses. ▶ The data processor handles/mitigates any vulnerabilities based on a risk assessment. ▶ The data processor has documented their handling/mitigation of weaknesses found.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's annual wheel and observed that the data processor performs annual penetration testing by external supplier. We have inspected that the data processor has had external penetration testing performed, and we observed that the data processor based on the results of the test has planned mitigated actions and documentation hereof.	No exceptions noted.

Article 28 (3)(c): Technical and organisational security measures

Control objectives

- *To ensure that the data processor has implemented appropriate technical and organisational security measures taking into account the actual technical level, implementation costs and the nature, scope, coherence, and purpose of the processing concerned as well as the risks of varying probability and gravity for natural persons rights and freedoms (risk assessment), including continuous examination and update of risk assessments and security measures.*
- *To ensure that the risk assessment takes into consideration risks of accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.*
- *To ensure confidentiality, integrity, and accessibility and robustness of processing systems and services.*
- *To ensure timely restoration of the accessibility of and access to personal data in case of a physical and technical incident.*
- *To ensure procedures for regular testing, assessment, and evaluation of the efficiency of the technical and organisational security measures to ensure the processing security.*

Control activity	Test performed by BDO	Result of test
Back-up and re-establishment of data ▶ Back-up of systems and data is performed daily. ▶ Operation and storage of backup are outsourced to subprocessor. ▶ Restore tests are performed twice a year.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's configuration of back-up and observed that backups of systems and data uploaded to the subprocessor Scaleway SAS are performed daily. We have inspected the subprocessor Scaleway SAS' ISO 27001 certification applicable until 14 February 2024 and through that derived that Scaleway has appropriate control measures in place in relation to back-up. We have inspected the data processor's annual wheel and observed that the data processor performs restore tests twice a year. The most recent test was performed in June 2023 and the next is planned for December 2023.	No exceptions noted.
Maintenance of system software ▶ Operating system software on servers and workstations is currently updated. ▶ The data processor has implemented a process for updating of system software for the purpose of ensuring system accessibility and security.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's procedure for updating system software and observed that it has been implemented. We have observed that automatic update of workstations and manual updating process for servers have been set up. We have inspected a selected work PC and observed that it has been updated.	No exceptions noted.

Article 28 (3)(c): Technical and organisational security measures

Control objectives

- *To ensure that the data processor has implemented appropriate technical and organisational security measures taking into account the actual technical level, implementation costs and the nature, scope, coherence, and purpose of the processing concerned as well as the risks of varying probability and gravity for natural persons rights and freedoms (risk assessment), including continuous examination and update of risk assessments and security measures.*
- *To ensure that the risk assessment takes into consideration risks of accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.*
- *To ensure confidentiality, integrity, and accessibility and robustness of processing systems and services.*
- *To ensure timely restoration of the accessibility of and access to personal data in case of a physical and technical incident.*
- *To ensure procedures for regular testing, assessment, and evaluation of the efficiency of the technical and organisational security measures to ensure the processing security.*

Control activity	Test performed by BDO	Result of test
	We have inspected a selected server and observed that it has been updated.	
Logging in systems, databases, and network, including logging of application of personal data - All successful and failed attempts to access the data processor's systems and data are logged. - All user changes in systems and databases are logged. - The log is deleted after the determined retention period. - The data processor monitors and logs network traffic. - The data processor stores logs for 6 months.	We have interviewed relevant personnel with the data processor. We have inspected documentation for that the data processor has set up logging of attempts to access the data processor's systems and data. We have inspected documentation for that the data processor has set up logging of user changes in the system. We have inspected documentation for that the data processor has set up logging of network traffic. We have inspected documentation of that logs are deleted and anonymised after 6 months.	No exceptions noted.
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 interviewed relevant personnel with the data processor. We have inspected that the data processor has established a monitor system for monitoring of production environments, including uptime, performance, and capacity, and we observed that the system generates notifications of alarms to the data processor.	No exceptions noted.

Article 28 (3)(c): Technical and organisational security measures

Control objectives

- *To ensure that the data processor has implemented appropriate technical and organisational security measures taking into account the actual technical level, implementation costs and the nature, scope, coherence, and purpose of the processing concerned as well as the risks of varying probability and gravity for natural persons rights and freedoms (risk assessment), including continuous examination and update of risk assessments and security measures.*
- *To ensure that the risk assessment takes into consideration risks of accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.*
- *To ensure confidentiality, integrity, and accessibility and robustness of processing systems and services.*
- *To ensure timely restoration of the accessibility of and access to personal data in case of a physical and technical incident.*
- *To ensure procedures for regular testing, assessment, and evaluation of the efficiency of the technical and organisational security measures to ensure the processing security.*

Control activity	Test performed by BDO	Result of test
Repair and service as well as disposal of IT equipment ▶ The data processor sends IT equipment for repair and service without it containing personal data. ▶ The data processor disposes of IT equipment by physical destruction of data-bearing media. ▶ The data processor securely deletes data on data-bearing media (overwriting/distortion, encryption). ▶ The data processor maintains a list of destroyed IT equipment.	We have interviewed relevant personnel with the data processor. we have inspected that the data processor has an overview of defect and destroyed IT equipment. We have inspected the data processor's conclusion of agreement with an external supplier on handling repair of defect IT equipment and disposal by physical destruction of data-bearing media. By inquiry, we have been informed that there has been no defect equipment since conclusion of the agreement with the external supplier, for which reason we were not able to test the control introduced.	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 data controller.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's annual wheel and observed that data processor tests, assesses, and evaluates the effectiveness of the technical and organisational security measures that are appropriate in relation to the data that is handled on behalf of the data controller.	No exceptions noted.

Article 28 (3)(c): Technical and organisational security measures

Control objectives

- *To ensure that the data processor has implemented appropriate technical and organisational security measures taking into account the actual technical level, implementation costs and the nature, scope, coherence, and purpose of the processing concerned as well as the risks of varying probability and gravity for natural persons rights and freedoms (risk assessment), including continuous examination and update of risk assessments and security measures.*
- *To ensure that the risk assessment takes into consideration risks of accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.*
- *To ensure confidentiality, integrity, and accessibility and robustness of processing systems and services.*
- *To ensure timely restoration of the accessibility of and access to personal data in case of a physical and technical incident.*
- *To ensure procedures for regular testing, assessment, and evaluation of the efficiency of the technical and organisational security measures to ensure the processing security.*

Control activity	Test performed by BDO	Result of test
	We have observed that the data processor completed the described control in March 2023.	

Article 25: Data protection through design and standard settings

Control objectives

- *To ensure that the data processor completes data protection via design and standard settings.*

Control activity	Test performed by BDO	Result of test
Development and Maintenance of systems ▶ The data processor works on privacy-by-design principles in development and maintenance tasks. ▶ At least once a year in connection with updating of the general risk assessment, it is assessed whether the data protection through design and standard settings in the established technical and organisational measures are appropriate.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's procedure regarding development and maintenance tasks, and we observed that the procedure deals with incorporation of privacy-by-design principles in development and maintenance tasks. We have observed that the data processor's development process includes requirements for the description of required development/maintenance in a ticket, in which the development is risk assessed in the protection of personal data. The subsequent quality assurance, tests, etc. are based on this risk assessment. The process also includes requirements for development, quality assurance, test, putting into service and roll-back. We have inspected a selected development task and observed that the requirements of the procedure have been complied with in the development process in question. We have inspected the data processor's annual wheel and observed that the data processor on an annual basis performs a general risk assessment, including assessment of the data protection through design and standard settings.	No exceptions noted.
Information security in development and changes ▶ The data processor works based on security-by-design principles in development and change tasks. ▶ A roll-back plan is implemented in case of errors in the production environment. ▶ At least once a year in connection with updating the general risk assessment, it is assessed whether the information security through design and development in	We have interviewed relevant personnel with the data processor. We have inspected the data processor's procedure regarding development and change tasks, and we observed that the procedure deals with incorporation of security-by-design principles in development and change tasks.	No exceptions noted.

Article 25: Data protection through design and standard settings		
Control objectives ▶ *To ensure that the data processor completes data protection via design and standard settings.*		
Control activity	**Test performed by BDO**	**Result of test**
the established technical and organisational measures are appropriate.	We have observed that the data processor's development process includes requirements for the description of required development/maintenance in a ticket, in which the development is risk assessed in IT security. The subsequent quality assurance, tests, etc. are based on this risk assessment. The process also includes requirements for development, quality assurance, test, putting into service and roll-back. We have inspected a selected development task and observed that the requirements of the procedure have been complied with in the development process in question. We have inspected the data processor's annual wheel and observed that the data processor on an annual basis performs a general risk assessment, including assessment of the information security through design and development.	
Segregation of development, test and production environments ▶ Segregation of duties between development and operation has been introduced. ▶ Changes to functionality are tested before put in operation. ▶ Development and test are performed in development environments, which are segregated from production systems. ▶ A version management system is used to register all changes in source code.	We have interviewed relevant personnel with the Processor. We have inspected whether there is segregation of duties between development and operation. We have inspected the development process and observed that it includes use of test before a new functionality is implemented. We have inspected the data processor's IT environments and observed that it is segregated from the production environment. We have inspected the data processor's version management system and observed that changes in the source code are recorded.	No exceptions noted.

Article 25: Data protection through design and standard settings		
Control objectives ▶ *To ensure that the data processor completes data protection via design and standard settings.*		
Control activity	**Test performed by BDO**	**Result of test**
	we have inspected a selected development task and observed that it has been developed in a separate development environment and has been test and put into service via a version management system.	
Personal data in development and test environments ▶ Anonymised test data are used in the development and test environments.	We have interviewed relevant personnel with the data processor. We have inspected the development environment and observed that the data processor has anonymised data in the development and test environment.	No exceptions noted.
Support assignments ▶ Supporters' access and handling of personal data is given based on support tickets and the supporters' work-related need.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's log of support cases and observed that support cases are processed based on support tickets. We have inspected documentation of that supporters with access to personal data have a work-related need. We have inspected the data processor's annual wheel and observed that the data processor reviews the supporters' access rights.	No exceptions noted.

Article 28 (3)(g): Deletion and return of personal data		
Control objectives ▶ *To ensure that the data processor can delete and return personal data after the termination of the service related to the processing in accordance with the data controller.*		
Control activity	**Test performed by BDO**	**Result of test**
Deletion of personal data ▶ The data processor deletes the data controller's personal data per instruction, at termination of the main agreement.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's general data processing agreement with data controllers and observed that the data processor is obligated to delete or return the data controller's personal data upon instruction, at termination of the main agreement. We have inspected that data have been deleted in the data processor's systems for the data processor's most recent terminated client.	No exceptions noted.
Return of personal data ▶ The data processor's system has a feature which ensure that terminated clients themselves may obtain their own data.	We have interviewed relevant personnel with the data processor. We have inspected that the data processor has set up a feature which ensure that terminated clients themselves may obtain their own data.	No exceptions noted.

Article 28 (3)(e)(f)(h): Assistance to the data controller		
Control objectives ▶ *To ensure that the data processor can assist the data controller with satisfying the data subjects' rights.* ▶ *To ensure that the data processor can assist the data controller in relation to security of processing (article 32), personal data breach (articles 33-34) and impact assessments (articles 35-36).* ▶ *To ensure that the data processor can assist the data controller in relation to audit and inspection.*		
Control activity	**Test performed by BDO**	**Result of test**
The data subjects' rights ▶ The data processor has prepared a procedure for assistance to the data controller at fulfilling the data subjects' rights. ▶ It is possible to provide insight into all information registered.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's procedure regarding assistance to data controllers and observed that it ensures assistance to the data controller at fulfilment of the data subjects' rights. By inquiry, we have been informed that there have been no requests regarding the data subjects' rights, for which reason we have not been able to test the procedure for implementation.	No exceptions noted.
Obligations of security of processing, personal data breach and impact assessments. ▶ Procedures have been prepared for assistance to the data controller when assisting in relation to articles 32-36.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's procedure for assistance to the data controller and observed that procedures have been prepared for assistance to the data controller when assisting in relation to articles 32-36. By inquiry, we have been informed that the data processor has not received requests regarding the data subjects' rights and the special requirements of the regulation, for which reason we have not been able to test the procedure for implementation.	No exceptions noted.
Audit and inspection ▶ The data processor is obligated to have prepared an ISAE 3000 assurance report on the technical and organisational security measures aimed at processing and protection of personal data.	We have interviewed relevant personnel with the Processor. We have inspected the data processor's concluded for data processing agreements and observed that the data processor is	No exceptions noted.

Article 28 (3)(e)(f)(h): Assistance to the data controller		
Control objectives ▶ *To ensure that the data processor can assist the data controller with satisfying the data subjects' rights.* ▶ *To ensure that the data processor can assist the data controller in relation to security of processing (article 32), personal data breach (articles 33-34) and impact assessments (articles 35-36).* ▶ *To ensure that the data processor can assist the data controller in relation to audit and inspection.*		
Control activity	**Test performed by BDO**	**Result of test**
▶ The data processor makes available the information necessary to the data controller and the supervisory authorities per request, in connection with audit and inspection of the Processor.	committed to have prepared an ISAE 3000 assurance report on the technical and organisational security measures aimed at processing and protection of personal data. We have prepared this ISAE 3000 assurance report for the data processor's obligation in this relation. We have observed that the data processor based on request from the data controller must be available for the data controller and make available the necessary information to the data controller and the supervisory authority in connection with audit and inspection of the data processor. By inquiry, we have been informed that during the last 12 months there has been a request from a data controller for providing information. We have inspected that the data processor has disclosed the necessary information to the data controller.	

Article 30 (2) (3) and (4): Record of categories of processing activities		
Control objectives ▶ *To ensure that the data processor prepares a written record of all the categories of processing activities carried out on behalf of the data controller.* ▶ *To ensure that the data processor stores the record in writing, including electronically.* ▶ *To ensure that the data processor can make available the record to the supervisory authority.*		
Control activity	**Test performed by BDO**	**Result of test**
Records of processing activities ▶ The Processor has established a record of processing activities as Processor. ▶ The record is updated with significant changes continuously. ▶ The record is updated at least once a year during the annual review.	We have interviewed relevant personnel with the Processor. We have inspected that the data processor has set up a record of processing activities as data processor. We have examined the data processor's annual wheel and observed that the data processor currently updates the record and at least once a year.	No exceptions noted.
Storage of the record ▶ The record is stored electronically in the data processor's system/file drive.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's record and observed that it is stored electronically in the data processor's file system.	No exceptions noted.
The Danish Data Protection Agency's access to the record ▶ The Processor hands over the record the request of the Danish Data Protection Agency.	We have interviewed relevant personnel with the Processor. We have inspected the data processor's procedure for providing the record of processing activities and observed that the data processor may provide the record to the Danish Data Protection Agency. By inquiry, we have been informed that the data processor has not received requests from the Danish Data Protection Agency regarding handing over the record, for which reason we we have not been able to test the implementation.	No exceptions noted.

Article 33 (2): Communication of personal data breach

Control objectives

- *To ensure that the data processor without undue delay notifies the data controller of personal data breaches.*
- *To ensure that the data controller will be notified of necessary information, so the breach may be assessed with a view to report it to the supervisory authority and communicate it to the data subject.*

Control activity	Test performed by BDO	Result of test
Communication of personal data breach ▶ The Processor communicates to the Controller the personal data breach without undue delay. ▶ The Processor updates the Controller on all information relevant and necessary, when the information is available to the Processor. ▶ Communication between data processor and data controller is documented and stored.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's procedure for data breach and notification of the data controller of the personal data breach, and we observed that it has been implemented. We observed that the procedure is concerned with update of the data controller with all relevant and necessary information and circumstances around documentation of the communication with the data controller. By inquiry, we have been informed that there have been no personal data breach since establishing the procedure, for which reason we have not been able to test for implementation.	No exceptions noted.
Identification of personal data breaches ▶ The data processor trains relevant staff in identification of personal data breaches. ▶ The data processor has prepared a procedure for assessing and identifying personal data breaches.	We have interviewed relevant personnel with the Processor. We have inspected documentation of that the data processor has trained relevant staff in identification of personal data breaches. We have inspected the data processor's procedure for data breaches and observed that their incident response includes a section about assessment and identification of data breaches.	No exceptions noted.

Article 33 (2): Communication of personal data breach

Control objectives

- *To ensure that the data processor without undue delay notifies the data controller of personal data breaches.*
- *To ensure that the data controller will be notified of necessary information, so the breach may be assessed with a view to report it to the supervisory authority and communicate it to the data subject.*

Control activity	Test performed by BDO	Result of test
Registration of personal data breaches ▶ The Processor registers personal data breaches in the data breach log. ▶ The Processor has prepared and implemented a procedure for experience gathering when personal data is breached.	We have interviewed relevant personnel with the Processor. We have inspected the data processor's procedure for data breach, including recording of personal data breaches in the data breach log, and we observed that it has been implemented. We observed that the procedure also deals with collection of past experience with personal data breaches. By inquiry, we have been informed that there have been no personal data breach since establishing the procedure, for which reason we have not been able to test for implementation.	No exceptions noted.

Articles 44-49: Transmission of personal data to third countries

Control objectives

- *To ensure that the data processor only transfers personal data to a third country or an international organisation when the provisions of articles 45-49 are complied with.*
- *To ensure that the data processor only transfers personal data in accordance with instructions from the data controller and in accordance with a valid transmission basis (articles 45-49).*

Control activity	Test performed by BDO	Result of test
Transmission of personal data to third countries ▶ Written procedures exist for the transfer of personal data to third countries or international organisations in accordance with the agreement with the data controller on the basis of a valid transfer basis. ▶ The data processor's procedure is reviewed and assessed on an ongoing basis, and at least once a year, whether the procedure needs to be updated.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's procedure for transmission of personal data to third countries or international organisations, and we observed that it is in accordance with the data processor's general data processing agreement. We have inspected the data processor's procedure and observed that the data processor's procedure is examined and assessed currently and at least once a year.	No exceptions noted.
Instructions from the data controller ▶ The data processor only transfers personal data to third countries or international organisations on the instructions of the data controller. ▶ The data processor documents instructions obtained regarding the transfer of personal data to third countries or international organisations from data controllers.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's general data processing agreement and observed that the data processor may only transfer data to third countries on instructions from the data controller. Further, we have observed that this instruction is documented in an appendix to the general data processing agreement.	No exceptions noted.
Valid transmission basis ▶ The Data Processor assesses and documents that a valid transfer basis exists in connection with the transfer of personal data to third countries or international organisations.	We have interviewed relevant personnel with the data processor. We have inspected the data processor's transfer impact assessment and observed that the data processor has assessed the transfer basis for an American subprocessor, Sendbird, Inc.	We have observed that the data processor uses an American-owned subprocessor and that the data processor does not have a valid transmission basis for transferring the data controller's personal data to the American subprocessor Sendbird, Inc. On 10 July 2023, the European Commission ruled that the so-called "EU-U.S. Data Privacy Framework" ensures a sufficient level of protection in connection with transmission of personal data from EU to USA and may thereby act a valid transmission basis.

Articles 44-49: Transmission of personal data to third countries

Control objectives

- *To ensure that the data processor only transfers personal data to a third country or an international organisation when the provisions of articles 45-49 are complied with.*
- *To ensure that the data processor only transfers personal data in accordance with instructions from the data controller and in accordance with a valid transmission basis (articles 45-49).*

Control activity	Test performed by BDO	Result of test
	We have inspected the data processor's overview of subprocessors and observed that the data processor applies a subprocessor in a third country. It is the American subprocessor Sendbird, Inc. On 10 July 2023, the European Commission ruled that the so-called "EU-U.S Data Privacy Framework" ensures a sufficient level of protection in connection with transmission of personal data from EU to USA and may thereby act a valid transmission basis. The ruling on sufficiency may however solely be used as transmission basis when transferring personal data to organisations in USA which have been certified under the EU-U.S. Data Privacy Framework with the American Commerce Department. We have checked whether Sendbird, Inc. is certified under the new transmission basis EU-U.S. Data Privacy Framework, which the European Commission entered on 10 July 2023 at 5 September 2023. We observed that Sendbird, Inc. does not have an active certificate, and thereby, the data processor does not have a valid transmission basis for transferring the data controller's personal data to the subprocessor Sendbird, Inc.	The ruling on sufficiency may however solely be used as transmission basis when transferring personal data to organisations in USA which have been certified under the EU-U.S. Data Privacy Framework with the American Commerce Department. The subprocessor Sendbird, Inc. did not have a valid certificate at 5 September 2023 and therefore did the subprocessor not have a valid transmission basis. No further exceptions noted.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

KYSTVEJEN 29
8000 AARHUS C

CVR-NR. 20 22 26 70