www.pwc.dk

The following is a translation of a Danish original document. Please note that the English translation is provided for convenience only. In case of any discrepancy, the Danish version shall prevail.

Itadel A/S

Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 1 January 2020 to 31 December 2020 pursuant to the data processing agreement with data controllers

February 2021

pwc

Contents

1. Management's statement

Itadel A/S processes personal data on behalf of data controllers in accordance with the data processing agreements.

The accompanying description has been prepared for data controllers who have used the hosting services and who have a sufficient understanding to consider the description along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the EU regulation on the "Protection of natural persons with regard to the processing of personal data and on the free movement of such data" and "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (subsequently "the data protection rules") have been complied with.

Itadel A/S uses B4Restore A/S as a subprocessor for backup services. This report uses the carve-out method and does not comprise controls that B4Restore A/S performs for Itadel A/S.

Itadel A/S confirms that:

a) The accompanying description in section 3 fairly presents the hosting services that have processed personal data for data controllers subject to the data protection rules throughout the period from 1 January 2020 to 31 December 2020. The criteria used in making this statement were that the accompanying description:

   (i) Presents how the hosting services were designed and implemented, including:

   - The types of services provided, including the type of personal data processed;
   - The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete and restrict 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 security measures 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;
   - Controls that we, in reference to the scope of the hosting services, have assumed would be implemented by the data controllers and which, if necessary in order to achieve the control objectives stated in the description, are identified in the description;
   - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the processing of personal data.

(ii) Includes relevant information about changes in the data processor's hosting services for the processing of personal data in the period from 1 January 2020 to 31 December 2020

(iii) Does not omit or distort information relevant to the scope of the hosting services being described for the processing of personal data while acknowledging that the description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the hosting services that the individual data controllers might consider important in their particular circumstances.

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 January 2020 to 31 December 2020. The criteria used in making this statement were that:

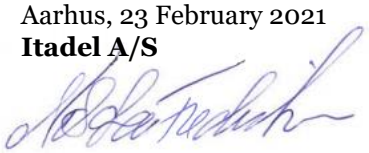
(i) The risks that threatened achievement of the control objectives stated in the description were identified;

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 January 2020 to 31 December 2020.

c) Appropriate technical and organisational measures were established and maintained to comply with the agreements with the data controllers, sound data processing practices and relevant requirements for data processors in accordance with the data protection rules.

Aarhus, 23 February 2021
Itadel A/S



Nils Lau Frederiksen
Information Security Manager, Itadel

2. Independent auditor's report

Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 1 January 2020 to 31 December 2020 pursuant to the data processing agreement with data controllers

To: Itadel A/S and Itadel A/S' customers

Scope

We have been engaged to provide assurance about Itadel A/S' description in section 3 of Itadel A/S' hosting services in accordance with the data processing agreement with data controllers throughout the period from 1 January 2020 to 31 December 2020 (the description) and about the design and operating effectiveness of controls related to the control objectives stated in the description.

Our report covers whether Itadel A/S has designed and effectively operated appropriate controls related to the control objectives stated in section 4. The report does not include an assessment of Itadel A/S' general compliance with the requirements of the EU regulation on the "Protection of natural persons with regard to the processing of personal data and on the free movement of such data" and "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (subsequently "the data protection rules").

Itadel A/S uses B4Restore A/S as a subprocessor for applied backup services. This report uses the carve-out method and does not comprise controls that B4Restore A/S performs for Itadel A/S.

We express reasonable assurance in our conclusion.

Itadel A/S' responsibilities

Itadel A/S is responsible for: preparing the description and accompanying statement in section 1, including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives and designing and effectively operating controls to achieve the stated control objectives.

Auditor's independence and quality control

We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by FSR – Danish Auditors, which are based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional conduct.

PricewaterhouseCoopers is subject to the International Standard on Quality Control (ISQC 1) and accordingly uses and maintains a comprehensive system of quality control, including documented policies and 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 Itadel A/S' description and on the design and operating effectiveness of controls related to the control objectives stated in that description, based on our procedures.

We conducted our engagement in accordance with ISAE 3000 (revised), "Assurance engagements other than audits or reviews of historical financial information", and additional requirements applicable in Denmark to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

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

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

Itadel A/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 hosting services that the individual data controllers may consider important in their particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect all personal data breaches. Furthermore, the projection of any evaluation of the operating effectiveness to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Opinion

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

a) The description fairly presents the hosting services as designed and implemented throughout the period from 1 January 2020 to 31 December 2020;

b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 January 2020 to 31 December 2020; and

c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 January 2020 to 31 December 2020.

Description of test of controls

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

Intended users and purpose

This report and the description of tests of controls in section 4 are intended only for data controllers who have used Itadel A/S' hosting services and who have a sufficient understanding to consider them, along with other information, including information about controls operated by the data controllers themselves, in assessing whether the requirements of the data protection rules have been complied with.

Aarhus, 23 February 2021
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab

Jesper Parsberg Madsen
State-Authorised Public Accountant

Iraj Bastar
Director

3. Description of processing

3.1 Description of hosting services

Introduction

Throughout the period from 1 January 2020 to 31 December 2020, controls regarding personal data have been established at Itadel with regard to the General Data Protection Regulation (GDPR). Thus, the technical and organisational controls have valid through the whole period. Procedures have been continuously implemented and updated to ensure that they comply with the GDPR and that they respect the advice and guidance of the Danish Data Protection Agency.

Description of Itadel

Itadel specialises in the outsourcing of IT operations. That means the operation of servers, platforms and applications as efficiently and securely as possible. This service is being provided on many platforms from five Danish data centres placed in Jutland and Zealand, of which the newest ones have been built as a 'Software-Defined Data Centre' (SDDC), which as standard is offered as a two-centre solution.

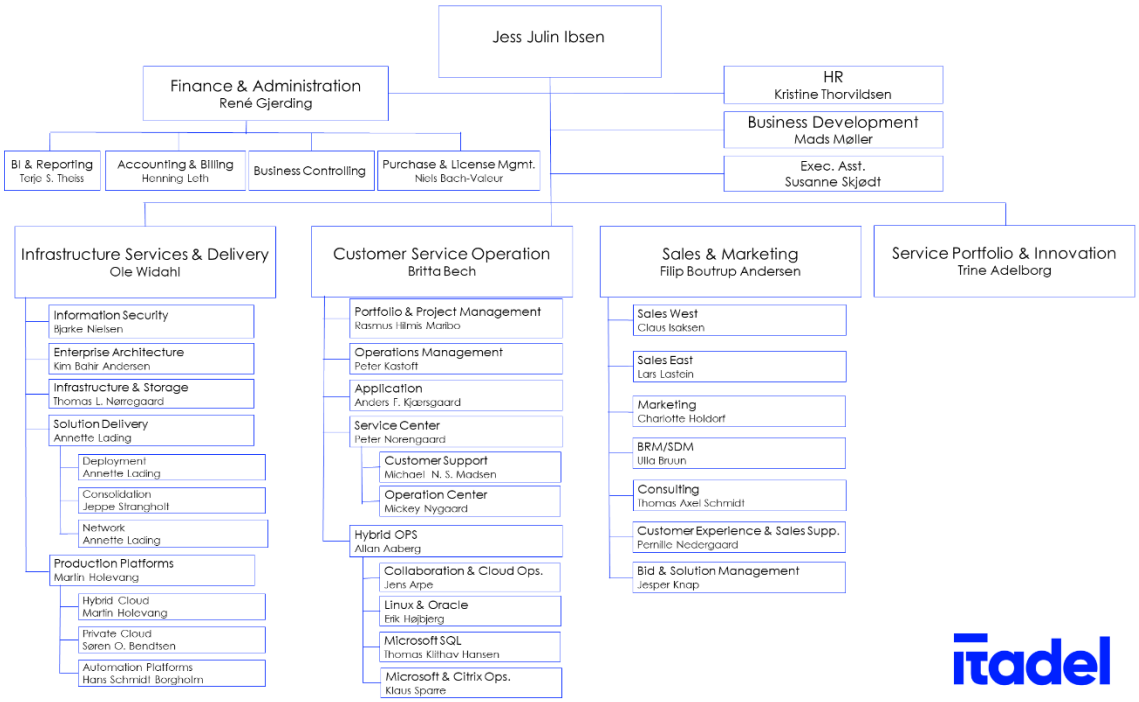
Itadel refers to the system description of the annual ISAE 3402 audit statement and to the Itadel website for a description of the services and offerings that Itadel provides.

Itadel is headquartered in Viby J (Aarhus, Denmark) with offices in Ballerup and in Prague in the Czech Republic.

Itadel currently employs 300 people, of which approximately 200 are technical personnel.

Itadel has an information security management system, which has been ISO 27001-certified since 2013.

Itadel is organised around key business areas that either directly provide professional service offerings or support these.



Organisation in regard to the GDPR

Bjarke Nielsen, Head of Information Security

Ebbe Skak Larsen, Chief Security Architect

Nils Lau Frederiksen, Information Security Manager (the Governance, Risk and Compliance team)

Morten Vinter Pedersen, Information Security Specialist

Rene Trusik, Cyber Analyst

Emmanuel Mung'ou Naibei, Cyber Analyst

Itadel does not have an appointed DPO (Data Protection Officer), but tasks relating to personal data and data processing are combined with the responsibility for IT and information security placed in the Information Security department.

Reporting to Management

Management of information security throughout all of Itadel is coordinated at the EMT meetings (Executive Management Team). Information Security continuously reports to the EMT regarding matters relating to both IT and information security as well as security regarding the processing of personal data.

The EMT decides on Itadel's policies regarding the securing of data in general and likewise ensures that procedures and instructions are implemented when necessary to achieve the goal of the policies. The EMT assesses the agreed policies at least once a year.

Compliance with the GDPR is seen as a natural part of everyday life and as a living part of the information security management system at Itadel.

Together with the ETM, risk assessments of matters of fundamental importance to information and data security are made continuously.

Technical and organisational measures

A more elaborate description of Itadel's technical and organisational systems can be found in the annual ISAE 3402 audit statement. This statement contains descriptions of internal processes, including IT processes regarding access management, incident management, problem management, capacity management, etc.

The ISAE 3402 audit statement is available in both Danish and English on Itadel's website:

https://www.itadel.dk/digitalisering/compliance-og-certificering

A more elaborate examination of the technical and organisational measures taken by Itadel to protect our own and our customers' data can be found on the following website:

https://www.itadel.dk/om-os/sikkerhed/databehandleraftale

How GDPR compliance is handled at Itadel

As for Itadel's compliance with the now former Danish data protection law (persondataloven) and the now enforced General Data Protection Regulation, the Information Security department is responsible for all visitation, handling and processing of all GDPR-related enquiries. More specifically, the Governance, Risk and Compliance team is handling the enquiries.

Processing of GDPR enquiries

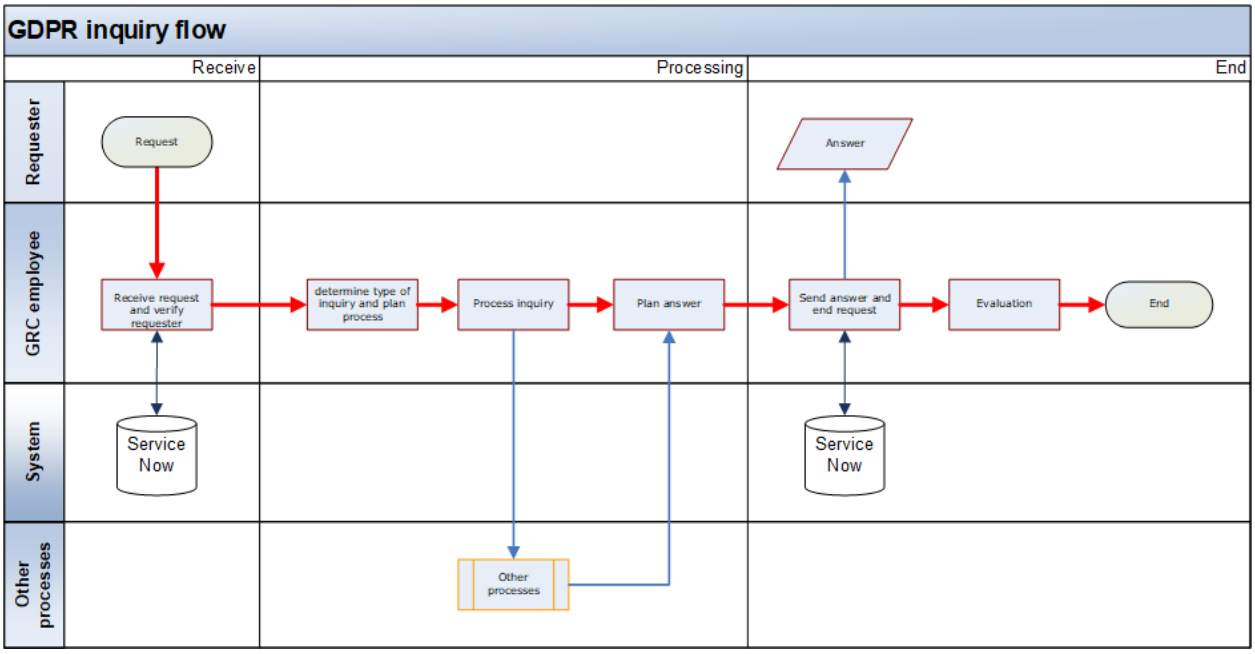
On Itadel's website, the principles in relation to the rights of the data subject are found:

https://www.itadel.dk/om-os/sikkerhed

To be able to assist the data controller in handling the rights of the data subjects, a dedicated mailbox has been set up (gdpr@itadel.dk). Itadel's employees, customers and sub-contractors will be able to contact Itadel via e-mail or via a ticket in Itadel's ITSM system. All enquiries can only be accessed by the Information Security department.

Itadel has a procedure for handling enquiries from the data controllers in relation to assisting with handling the rights of the data subjects (access, erasure, rectification, etc.).

All enquiries are processed within 30 days via the actions shown below in the flow chart diagram:



Employee awareness in relation to the GDPR

Up to, under and after the implementation of the GDPR at Itadel, it has regularly been communicated to the employees how to handle personal data in the future. Even though only a relatively small number of employees handle personal data on a daily basis, there has been a widespread awareness regarding personal data amongst all Itadel employees.

All employees receive thorough training in Itadel's information security rules when they start at Itadel as well as regular updates regarding information security on Itadel's intranet and news site.

Every month, knowledge about current threats against Itadel is published via blogposts and posters at Itadel.

It is the responsibility of the employees to comply with the policies and guidelines in force at any time.

Data processing agreements

When relevant, Itadel secures an approved data processing agreement whenever new customers are brought into Itadel.

The same happens when entering into a sub-processing agreement with sub-processors. Even though it is the responsibility of the data controller to make specific demands, Itadel has taken on the role of securing a data processing agreement with all Itadel's customers and suppliers.

Supervision with sub-processors

Itadel regularly monitors approved sub-processors. This is done by demanding either IT audit reports (ISAE 3402 and/or ISAE 3000) carried out by an impartial third party or by a pre-agreed visit and subsequent audit at the processor. Itadel demands the above-mentioned ISAE audit reports every year and if Itadel does not receive them, Itadel will take a risk-based approach and visit the processor to ensure they are compliant.

Itadel's approved processors can be found on the following site:

https://www.itadel.dk/om-os/sikkerhed/sub-processors

Categories of personal data collected, processed and stored

As a data processor (Itadel) for the data controller (customer), Itadel only collects, processes and stores personal data at the data controller's request. This matter and the categories of personal data are further agreed in the specific data processing agreements entered into by Itadel and the customers.

Categories of personal data are primarily found in applications (customer systems).

Itadel has not and does not need access to these systems when it comes to bug fixes and operational matters.

Itadel has made a list over internal systems in which personal data are processed and stored. The personal data are updated and deleted whenever there are changes in the workforce and in accordance with the demands of the GDPR and the Danish Bookkeeping Act.

Transfer to third countries

Unless otherwise agreed in the customer's specific data processing agreement, personal data will not be sent to third countries outside the European Union. Itadel has five data centres in Denmark and only makes use of public cloud hosting via European nodes in our delivery of public cloud.

Handling of security breaches

In case of an actual security breach in a customer system and/or in an internal system where personal data is processed, a ticket will be opened in Itadel's Service Management system. Within the timeframes agreed with the customer, Itadel then informs the customer about the nature of the security breach, the size and the preliminary extent with regards to a possible personal data breach at Itadel or the customer.

If Itadel is processing personal data on behalf of and is following instructions from the data controller and a personal data breach occurs, Itadel will assist in assuming:

- the responsibility of reporting a personal data breach to the controlling authority (the Danish Data Protection Agency) without undue delay and, where feasible, no later than 72 hours after having become aware of the security breach unless the personal data breach is unlikely to result in a risk to the rights and the freedoms of natural persons

- the responsibility to inform the data subject(s) about the personal data breach without undue delay when a personal data breach involves a high risk to the rights and freedoms of natural persons

- the responsibility to confer with the controlling authority (the Danish Data Protection Agency) before processing if an impact assessment regarding data protection shows that the processing will result in a high risk because of the arrangements made by the data controller to minimise the risk.

3.2 Complementary controls at the data controllers

Here, a description is made of areas in which the data controller has the primary responsibility for e.g. giving Itadel instructions and handle requests from data subjects regarding their rights. The data controller must:

- Consider the consequences related to the protection of personal data when change requests are raised
- Ensure that personal data are not included in support cases
- Warrant that the purpose of the processing of personal data is lawful and fair and that Itadel is only provided with the personal data necessary to fulfil the purpose
- Be responsible for ensuring that a legal basis for processing exists at the time of the transfer of the personal data to Itadel – including that any consent is freely given, specific, informed, unambiguous as well as explicit, if required
- Warrant that the individuals to whom the personal data relate (the data subjects) have been sufficiently informed about the processing of their personal data
- Have the primary responsibility for giving Itadel instructions about data processing and handle requests from data subjects regarding their rights
- Report any personal data breaches to the Danish Data Protection Agency.

4. Control objectives, control activities, tests and test results

4.1 Purpose and scope

We have conducted our engagement in accordance with ISAE 3000, Assurance engagements other than audits or reviews of historical financial information and additional requirements under Danish audit regulation.

Our testing of the design, implementation and functionality of the controls has included the control objectives and related control activities selected by Management and listed in section 4.3. Any other control objectives, related controls and controls at the affiliated enterprises are not covered by our test actions.

Our operating effectiveness testing included the control activities deemed necessary to obtain reasonable assurance that the stated control activities were achieved in the period from 1 January 2020 to 31 December 2020.

4.2 Test actions performed

The test actions performed when determining the operating effectiveness of the control activities are described below:

Inspection	Reading of documents and reports containing specifications regarding the execution of the control. This includes reading and consideration of reports and other documentation in order to assess whether specific controls are designed so they may be expected to become effective, if implemented. Furthermore, it is assessed whether controls are being monitored and checked sufficiently and at appropriate intervals. We have tested the specific system set-up on the technical platforms, databases and network components in order to verify whether controls are implemented and have functioned in the period from 1 January 2020 to 31 December 2020. Among other things, this includes assessment of patching level, permitted services, segmentation, password complexity, etc. as well as inspection of equipment and locations.
Inquiries	Inquiries of relevant personnel. Inquiries have included how the controls are performed.
Observation	We have observed the execution of the control.
Reperformance of the control	Repetition of the relevant control. We have repeated the execution of the control to verify that the control functions as assumed.

4.3 Control objectives, control activities, tests and test results

Principles relating to processing of personal data (Article 5)

Control objective:

Procedures and controls are followed to ensure that the collection, processing and storage of personal data take place in accordance with the principles relating to processing of personal data.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	There are written procedures in which a decision has been made on the following principles related to the processing of personal data: • Lawfulness, fairness and transparency • Purpose limitation • Data minimisation • Accuracy • Storage limitation • Integrity and confidentiality. A regular – at least annual – assessment is carried out as to whether to update these procedures.	Inspected that there are updated written procedures for the processing of personal data that include principles related to the processing of personal data.	No exceptions noted.
2	A regular – at least annual – assessment is carried out as to whether principles related to the processing of personal data are being complied with, and this assessment is documented.	Inspected documentation of the assessment of principles related to the processing of personal data in order to ensure that an assessment of principles for the processing of personal data and compliance with these is carried out at least annually.	No exceptions noted.
3	Management has dealt with and approved the assessment of compliance with the principles related to the processing of personal data.	Inspected documentation of Management's approval of the assessment of compliance with the principles for processing of personal data.	No exceptions noted.

Lawfulness of processing (Article 6)

Control objective:

Procedures and controls are followed to ensure that personal data are only processed lawfully.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	There are written procedures that contain requirements that personal data must only be processed where there is a lawful basis. A regular – at least annual – assessment is carried out as to whether to update these procedures.	Inspected that there are updated written procedures for the processing of personal data that contain requirements for the lawful processing of personal data.	No exceptions noted.
2	There is a data processing agreement or suchlike approved by the data controller and containing a summary of the basis on which the processing of personal data is carried out.	Inspected documentation stating the basis on which the processing of personal data is carried out and that this is approved by the data controller (data processing agreement etc.).	No exceptions noted.
3	A regular – at least annual – update is carried out of the statement by the data controller of the basis on which the processing of personal data is carried out.	Inspected documentation stating that the statement of the basis for processing of personal data has been updated and approved by the data controller at least annually.	No exceptions noted.
4	A regular – at least annual – assessment is carried out that there has been no unlawful processing of personal data, and this assessment is documented.	Inspected documentation of a regular – at least annual – assessment that there is no and has been no unlawful processing of personal data.	No exceptions noted.
5	Management has dealt with and approved the assessment of whether there has been any unlawful processing of personal data.	Inspected documentation of Management's approval of the assessment of whether there has been any unlawful processing of personal data.	No exceptions noted.

Conditions for consent (Articles 7 and 8)

Control objective:

Procedures and controls are followed to ensure that personal data is processed with the prior written consent of data subjects.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	There are written procedures for obtaining written consent to the processing of personal data. A regular – at least annual – assessment is carried out as to whether to update these procedures.	The company is not responsible for consent related activities and the controls are not applicable.	No exceptions noted.
2	A regular – at least annual – control is carried out that written consent to the processing of personal data has been obtained.	The company is not responsible for consent related activities and the controls are not applicable.	No exceptions noted.
3	Management has dealt with and approved the control describing that written consent to the processing of personal data has been obtained.	The company is not responsible for consent related activities and the controls are not applicable.	No exceptions noted.

Processing of special categories of personal data (Articles 9 and 10)

Control objective:

Procedures and controls are followed to ensure that the processing of special categories of personal data only takes place with consideration to established criteria, conditions and the appropriate safeguards.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	There are written procedures in which it is decided that the processing of special categories of personal data must only take place at the data processor if the criteria for processing are specifically agreed with the individual data controller. A regular – at least annual – assessment is carried out as to whether to update these procedures.	Inspected that there are updated written procedures in which it is decided that the processing of special categories of personal data at the data processor must only take place if the criteria for processing is specifically agreed with the data controller.	No exceptions noted.
2	There is a data processing agreement or suchlike approved by the data controller that contains an updated statement of the basis on which the processing of special categories of personal data is carried out.	Inspected documentation stating that the processing of special categories of personal data is carried out on the basis approved by the data controller.	No exceptions noted.
3	A regular – at least annual – assessment is carried out as to whether special categories of personal data have been processed without prior instructions from the data controller.	Inspected documentation of assessment of whether special categories of personal data have been processed without prior instructions from the data controller.	No exceptions noted.
4	Management has dealt with and approved the assessment of whether the requirements for processing special categories of personal data have been complied with.	Inspected documentation of Management's approval of the assessment of whether the requirements for processing special categories of personal data have been complied with.	No exceptions noted.

Processing which does not require identification (Article 11)

Control objective:

Procedures and controls are followed to ensure that storage, collection and processing of information to identify the data subject are maintained as long as identification is required.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	There are written procedures to ensure that storage, collection and processing of information to identify the data subject are maintained as long as identification is required. A regular – at least annual – assessment is carried out as to whether to update these procedures.	Inspected that there are updated written procedures ensuring that storage, collection and processing of information to identify the data subject are maintained as long as identification is required.	No exceptions noted.
2	There is an overview of criteria for storage, collection and processing of information to identify the data subject, which is approved by the data controller.	Inspected documentation stating that the criteria for storage, collection and processing of information to identify the data subject have been approved by the data controller.	No exceptions noted.
3	There is a regular – at least annual – update of the overview of criteria for storage, collection and processing of information to identify the data subject, approved by the data controller.	Inspected documentation stating that there is a regular – at least annual – update of the overview of criteria for storage, collection and processing of information to identify the data subject, approved by the data controller.	No exceptions noted.
4	There is a regular – at least annual – assessment that the storage, collection and processing of information to identify the data subject meet the criteria set out by the data controller.	Inspected documentation stating that the storage, collection and processing of information to identify the data subject meet the criteria set out by the data controller.	No exceptions noted.
5	Management has dealt with and approved the assessment as to whether the storage, collection and processing of information to identify the data subject meet the criteria set out by the data controller.	Inspected documentation stating that Management has approved the assessment as to whether the storage, collection and processing of information to identify the data subject are carried out as long as required by the criteria approved by the data controller.	No exceptions noted.

Transparent information, communication and modalities for the exercise of the rights of the data subject (Article 12)

Control objective:

Procedures and controls are followed to ensure that information on the processing of personal data can be provided to the data subject in a transparent, easily accessible and intelligible form.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	There are written procedures describing how to ensure that information on the processing of personal data can be provided to the data subject or how the data processor can assist the data controller with this. A regular – at least annual – assessment is carried out as to whether to update these procedures.	Inspected that there are updated written procedures describing how to ensure that information on the processing of personal data can be provided to the data subject or the data controller.	No exceptions noted.
2	There is an updated description of the information on the processing of personal data, which is approved by the data controller.	Inspected the description of the information on the processing of personal data to ensure that the information is provided to the data subject in a transparent, easily accessible and intelligible form. Inspected that the description of the information on the processing of personal data is updated and approved by the data controller.	No exceptions noted.
3	Management has ensured that the information on the processing of personal data is updated and approved by the data controller.	Inspected documentation stating that Management has ensured that the information on the processing of personal data is updated and approved by the data controller.	No exceptions noted.
4	There are written procedures describing how to ensure that replies to the data subject's requests and reasons for any rejection are made in a timely manner or how the data processor can assist the data controller with this. A regular – at least annual – assessment is carried out as to whether to update these procedures.	Inspected that there are updated written procedures describing how to ensure that replies to the data subject's requests and reasons for any rejection are made in a timely manner.	No exceptions noted.
5	It is regularly – at least annually – ensured that replies to the data subjects' requests have been made in a timely manner.	Inspected documentation stating that actual replies to data subjects' requests have been made in a timely manner and according to procedures.	No exceptions noted.

Control objective:

Procedures and controls are followed to ensure that information on the processing of personal data can be provided to the data subject in a transparent, easily accessible and intelligible form.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
6	Management has ensured that replies to data subjects' requests and reasons for any rejection are handled in an appropriate and timely manner.	Inspected documentation stating that Management has ensured that replies are handled in an appropriate and timely manner.	No exceptions noted.

Information to be provided where personal data are collected from the data subject (Articles 13 and 14)

Control objective:

Procedures and controls are followed to ensure that the data subject has received the data controller's contact details, information on the purpose of processing the personal data and information on any transfer of personal data to recipients, third countries or international organisations.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	There are written procedures describing how to ensure that the data subject receives information on the purpose of processing the personal data and information on any transfer of personal data to recipients, third countries or international organisations or how the data processor can assist the data controller with this. A regular – at least annual – assessment is carried out as to whether to update these procedures.	The company is not responsible for providing information to the data subjects, and the controls are not applicable.	No exceptions noted.
2	There is an updated description of the information on the data processor's processing of personal data etc. which is approved by the data controller.	The company is not responsible for providing information to the data subjects, and the controls are not applicable.	No exceptions noted.
3	Management has ensured that the description of the information on the data processor's processing of personal data etc. is updated and approved by the data controller.	The company is not responsible for providing information to the data subjects, and the controls are not applicable.	No exceptions noted.
4	There are written procedures describing the provision of information to the data subject on the right to access, rectify or erase personal data as well as to restrict the processing of personal data, or how the data processor can assist the data controller with this. A regular – at least annual – assessment is carried out as to whether to update these procedures.	The company is not responsible for providing information to the data subjects, and the controls are not applicable.	No exceptions noted.
5	There is an updated description of the data subject's right to access, rectify, erase, etc. personal data, which is approved by the data controller.	The company is not responsible for providing information to the data subjects, and the controls are not applicable.	No exceptions noted.
6	A regular – at least annual – control is carried out that all data subjects have received the description of the data subject's right to access, rectify or erase personal data.	The company is not responsible for providing information to the data subjects, and the controls are not applicable.	No exceptions noted.

Control objective:

Procedures and controls are followed to ensure that the data subject has received the data controller's contact details, information on the purpose of processing the personal data and information on any transfer of personal data to recipients, third countries or international organisations.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
7	Management has ensured that the description of the information on the data subject's right to access, rectify etc. is updated and approved by the data controller and that it is communicated to all data subjects.	The company is not responsible for providing information to the data subjects, and the controls are not applicable.	No exceptions noted.

Right of access by the data subject (Article 15)

Control objective:

Procedures and controls are followed to ensure that the data subject's right to access his own registered personal data and the processing of this are complied with.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	There are written procedures describing how data subjects' requests to access their own registered personal data are handled, or how the data processor can assist the data controller with this. A regular – at least annual – assessment is carried out as to whether to update these procedures.	Inspected that there are written procedures describing how data subjects' requests to access their own registered personal data are handled.	No exceptions noted.
2	The data processor has prepared a description to the data subject on how personal data is collected, processed and stored, which is approved by the data controller.	Inspected documentation stating that the description of how personal data is collected, processed and stored is approved by the data controller.	No exceptions noted.
3	The data processor has an established defined format for the extraction of personal data (copy of the personal data registered and processed) to the data subject, which is approved by the data controller.	Inspected documentation stating that the content of the extraction of personal data is approved by the data controller.	No exceptions noted.
4	A regular – at least annual – assessment is carried out as to whether the extraction of personal data to the data subject and the description of how the personal data will be processed is updated and correct.	Inspected documentation stating that the extraction of personal data to the data subject and the description of how the personal data will be processed is updated and correct.	No exceptions noted.
5	It is regularly – at least annually – ensured that replies to the data subjects' requests have been made in a timely manner.	Inspected documentation that actual replies to data subjects' requests have been made in a timely manner and according to procedures.	No exceptions noted.
6	Management has ensured that the extraction of personal data and the description of how the personal data will be processed are updated and correct and approved by the data controller, and that requests are handled in a timely manner.	Inspected documentation stating that Management has ensured that the extraction of personal data and the description of how the personal data will be processed is updated and correct and approved by the data controller, and that requests are handled in a timely manner.	No exceptions noted.

Right to rectification (Articles 16 and 19)

Control objective:

Procedures and controls are followed to ensure that the data subject's right to rectification of his own registered personal data is complied with, including rectification at recipients of the personal data.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	There are written procedures describing the handling of data subjects' right to rectification of personal data, or how the data processor can assist the data controller with this. A regular – at least annual – assessment is carried out as to whether to update these procedures.	Inspected that there are updated written procedures for the handling of data subjects' right to rectification of personal data.	No exceptions noted.
2	Technical measures have been established in the IT systems used in order to ensure that personal data can be rectified.	Inspected documentation stating that technical measures have been established in the IT systems used in order to rectify personal data. Inspected documentation stating that personal data are only rectified by means of the established technical measures.	No exceptions noted.
3	A regular – at least annual – assessment is carried out that the rectification of personal data has taken place correctly and without undue delay.	Inspected documentation of control describing that the rectification of personal data has taken place correctly and without undue delay.	No exceptions noted.
4	Management has dealt with and approved the assessment that the rectification of personal data has taken place correctly and without undue delay.	Inspected documentation stating that Management has ensured that the rectification of personal data has taken place correctly and without undue delay.	No exceptions noted.

Right to erasure ('right to be forgotten') (Articles 17 and 19)

Control objective:

Procedures and controls are followed to ensure that the data subject's right to erasure of his own registered personal data is complied with, including erasure at recipients of the personal data.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	There are written procedures describing the handling of data subjects' right to erasure of personal data, or how the data processor can assist the data controller with this. A regular – at least annual – assessment is carried out as to whether to update these procedures.	Inspected that there are updated written procedures for the handling of data subjects' right to erasure of personal data.	No exceptions noted.
2	Technical measures have been established in the IT systems used in order to ensure that personal data can be erased.	Inspected documentation stating that technical measures have been established in the IT systems used in order to erase personal data. Inspected documentation stating that personal data are only erased by means of the established technical measures.	No exceptions noted.
3	A regular – at least annual – assessment is carried out that the erasure of personal data has taken place correctly and without undue delay.	Inspected documentation of control describing that the erasure of personal data has taken place correctly and without undue delay.	No exceptions noted.
4	Management has dealt with and approved the assessment as to whether the erasure of personal data has taken place correctly and without undue delay.	Inspected documentation stating that Management has ensured that the erasure of personal data has taken place correctly and without undue delay.	No exceptions noted.

Right to restriction of processing (Articles 18 and 19)

Control objective:

Procedures and controls are followed to ensure that the data subject's right to restriction of processing of his own registered personal data is complied with, including restriction at recipients of the personal data.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	There are written procedures describing the handling of data subjects' right to restriction of processing of personal data, or how the data processor can assist the data controller with this. A regular – at least annual – assessment is carried out as to whether to update these procedures.	Inspected that there are updated written procedures for the handling of data subjects' right to restriction of processing of personal data.	No exceptions noted.
2	Technical measures have been established in the IT systems used in order to ensure that the processing of personal data can be restricted.	Inspected documentation stating that technical measures have been established in the IT systems used in order to restrict the processing of personal data. Inspected documentation stating that the processing of personal data is only restricted by means of the established technical measures.	No exceptions noted.
3	A regular – at least annual – assessment is carried out that the restriction of the processing of personal data takes place correctly and without undue delay.	Inspected documentation of control describing that the restriction of the processing of personal data has taken place correctly and without undue delay.	No exceptions noted.
4	Management has dealt with and approved the assessment as to whether the restriction of the processing of personal data has taken place correctly and without undue delay.	Inspected documentation stating that Management has ensured that the restriction of the processing of personal data has taken place correctly and without undue delay.	No exceptions noted.

Right to data portability (Article 20)

Control objective:

Procedures and controls are followed to ensure that the data subject's right to transfer his own registered personal data to another data controller is complied with.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	There are written procedures describing how the data subject's right to transfer his own registered personal data to another data controller is dealt with, or how the processor can assist the data controller with this. A regular – at least annual – assessment is carried out as to whether to update these procedures.	Inspected that there are updated written procedures for dealing with the data subject's right to transfer his own registered personal data to another data controller.	No exceptions noted.
2	Technical measures have been established in the IT systems used in order to ensure it is possible to transfer personal data.	Inspected documentation stating that technical measures have been established in the IT systems used to ensure it is possible to transfer personal data. Inspected documentation stating that the transfer of personal data only takes place by means of the technical measures.	No exceptions noted.
3	The data processor has an established defined format for extracts of personal data (copy of the personal data registered and processed) to the data subject or another data controller/processor, which is approved by the data controller.	Inspected documentation stating that the extraction of personal data for transfer is approved by the data controller.	No exceptions noted.
4	There is a regular – at least annual – assessment that the transfer of personal data takes place correctly and without undue delay.	Inspected documentation stating that the transfer of personal data has taken place correctly and without undue delay.	No exceptions noted.
5	Management has dealt with and approved the assessment that the transfer of personal data has taken place correctly and without undue delay.	Inspected documentation stating that Management has ensured that the transfer of personal data has taken place correctly and without undue delay.	No exceptions noted.

Responsibility of the data controller – implementation of appropriate data protection (Article 24)

Control objective:

Procedures and controls are followed to ensure that technical and organisational measures for safeguarding the rights of the data subject and the processing of personal data function in accordance with the data controller's guidance.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	The data processor has received instructions for the processing and protection of personal data from the data controller.	Inspected documentation stating that the data controller has given the data processor instructions on the processing and protection of personal data.	No exceptions noted.
2	The processor has general written procedures, including a description of the technical and organisational measures to safeguard the data subject's rights and the processing of personal data, which are approved by the data controller.	Inspected documentation stating that the data controller has approved the processor's general written procedures, including technical and organisational measures to safeguard the data subject's rights and the processing of personal data.	No exceptions noted.
3	The data processor has prepared a description of the use of sub-processors, including a description of the sub-processors' technical and organisational measures to protect the rights of the data subject and the processing of personal data, which are approved by the data controller.	Inspected documentation stating that the data controller has approved the data processor's sub-processors, including their technical and organisational measures to safeguard the data subject's rights and the processing of personal data.	No exceptions noted.
4	There is a regular – at least annual – assessment that the safeguarding of the rights of the data subject and the processing of personal data have taken place in accordance with the instructions from the data controller and the approved procedures.	Inspected documentation of control describing that the safeguarding of the rights of the data subject and the processing of personal data have taken place in accordance with the instructions and approved procedures.	No exceptions noted.
5	Management has dealt with and approved the assessment that the safeguarding of the rights of the data subject and the processing of personal data have taken place in accordance with the instructions from the data controller and the approved procedures.	Inspected documentation stating that Management has ensured that the safeguarding of the rights of the data subject and the processing of personal data have taken place in accordance with the instructions from the data controller and the approved procedures.	No exceptions noted.

Data protection by design and by default (Article 25)

Control objective:

Procedures and controls are followed to ensure that the requirements for data protection by design and by default in the data processor's technical and organisational security measures function effectively.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	There are written procedures describing data protection by design and by default, including how the data processor can assist the data controller in the safeguarding of this. A regular – at least annual – assessment is carried out as to whether to update these procedures.	Inspected that there are updated written procedures describing data protection by design and by default, including how the data processor can assist the data controller in the safeguarding of this.	No exceptions noted.
2	The processor has established technical and organisational security measures corresponding to the data controller's requirement for technical and organisational security measures and data protection, such as pseudonymisation and data minimisation etc.	Inspected documentation stating that the technical and organisational security measures corresponding to the data controller's requirement for technical and organisational security measures and data protection have been established. Inspected documentation stating that the established technical and organisational security measures have been efficient during the report period.	No exceptions noted.
3	The technical and organisational security measures established by the data processor are approved by the data controller.	Inspected documentation stating that the data controller has approved the established technical and organisational security measures.	No exceptions noted.
4	There is a regular – at least annual – assessment that technical and organisational security measures and the data protection are in accordance with the data controller's requirements for this.	Inspected documentation of control that the technical and organisational security measures and data protection are in accordance with the data controller's requirements for this.	No exceptions noted.
5	The data processor has received instructions from the data controller regarding which personal data are necessary (data minimisation) and how these must be processed in relation to the individual specific purpose of processing.	Inspected documentation of the data controller's instructions to the data processor regarding which personal data are necessary and how these must be processed in relation to the specific purpose of processing.	No exceptions noted.

Control objective:

Procedures and controls are followed to ensure that the requirements for data protection by design and by default in the data processor's technical and organisational security measures function effectively.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
6	There is a regular – at least annual – assessment that only the personal data necessary in relation to the individual specific purpose of processing and the instructions received are processed.	Inspected documentation of control that the processing of personal data is restricted to the specific purpose in accordance with instructions.	No exceptions noted.
7	Management has dealt with and approved the assessment that the technical and organisational security measures and data protection are ensured, and that the processing of personal data has taken place in accordance with requirements and instructions from the data controller and with the approved procedures.	Inspected documentation stating that Management has ensured that the technical and organisational security measures, data protection and processing of personal data have taken place in accordance with the requirements and instructions from the data controller and with the approved procedures.	No exceptions noted.

Data processor – processing of personal data under the authority of the data controller (Articles 28 and 29)

Control objective:

Procedures and controls are followed to ensure that the processing of personal data only takes place in accordance with a contract or other legally binding document (data processing agreement) and that data processing is only carried out by data processors approved by the data controller.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	A contract or other legally binding document (data processing agreement) has been entered into between the data processor and the data controller that describes the technical and organisational security measures established by the data processor so that the data processing fulfils the requirements of the Data Protection Regulation and the Data Protection Act and ensures protection of the rights of the data subject.	Inspected documentation stating that the data processing agreement describes the technical and organisational security measures established by the data processor so that the data processing fulfils the requirements of the Data Protection Regulation and the Data Protection Act and ensures protection of the rights of the data subject.	No exceptions noted.
2	The data processor has received a specific or general approval by the data controller of the use of other sub-processors. In case of a general written approval, the data processor must notify the data controller of any planned changes in terms of addition or replacement of sub-processors.	Inspected documentation stating that the data controller has approved the use of other sub-processors. Inspected documentation stating that the data controller has been notified of planned changes in terms of addition or replacement of sub-processors.	No exceptions noted.
3	The data processor has received the data controller's instructions for the processing and protection of personal data at the data processor.	Inspected documentation stating that the data controller has given the data processor instructions on the processing and protection of personal data.	No exceptions noted.
4	There are written procedures describing that only the data processor may process personal data, including transferring personal data to a third country or international organisation, in accordance with documented instructions from the data controller in relation to European Union law or national law. A regular – at least annual – assessment is carried out as to whether to update these procedures.	Inspected that there are updated written procedures describing that only the data processor may process and transfer personal data in accordance with documented instructions from the data controller or pursuant to European Union law or national law.	No exceptions noted.

Control objective:

Procedures and controls are followed to ensure that the processing of personal data only takes place in accordance with a contract or other legally binding document (data processing agreement) and that data processing is only carried out by data processors approved by the data controller.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
5	There are written procedures describing that the data processor will ensure that the persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of secrecy. A regular – at least annual – assessment is carried out as to whether to update these procedures.	Inspected that there are updated written procedures describing that the persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of secrecy.	No exceptions noted.
6	When the data processor makes use of sub-processors for specific processing activities on behalf of the data controller, there are written procedures describing the data processor's controls to ensure that the sub-processor complies with the same data processing obligations as those defined in the data processing agreement between the data controller and the data processor. A regular – at least annual – assessment is carried out as to whether to update these procedures.	Inspected that there are updated written procedures describing the data processor's controls to ensure that sub-processors comply with the same data processing obligations as those defined in the data processing agreement between the data controller and the data processor.	No exceptions noted.
7	There are written procedures describing how the data processor assists the data controller as far as possible with fulfilling the data controller's obligation to respond to requests to exercise the data subjects' rights by means of appropriate technical and organisational measures. A regular – at least annual – assessment is carried out as to whether to update these procedures.	Inspected that there are updated written procedures describing how the data processor assists the data controller in performing his or her obligation to respond to requests relating to the exercise of the data subjects' rights by means of appropriate technical and organisational measures.	No exceptions noted.
8	There are written procedures describing how the data processor – taking into account the nature of the processing and the information available to the processor – can assist the data controller in complying with the data controller's obligations in relation to: • Security of processing (Article 32) • Notification of a personal data breach to the supervisory authority (Article 33)	Inspected that there are updated written procedures describing how the data processor assists the data controller with ensuring compliance with the data controller's obligations.	No exceptions noted.

Control objective:

Procedures and controls are followed to ensure that the processing of personal data only takes place in accordance with a contract or other legally binding document (data processing agreement) and that data processing is only carried out by data processors approved by the data controller.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
	• Communication of a personal data breach to the data subject (Article 34) • Data protection impact assessment (Article 35) • Prior consultation (Article 36). A regular – at least annual – assessment is carried out as to whether to update these procedures.		
9	There are written procedures describing how the data processor, at the choice of the data controller, erases or returns all the personal data to the data controller after the end of the provision of services relating to processing, and erases existing copies unless European Union or Member State law requires storage of the personal data. A regular – at least annual – assessment is carried out as to whether to update these procedures.	Inspected that there are updated written procedures describing how the data processor, at the choice of the data controller, erases or returns all the personal data to the data controller after the end of the provision of services relating to processing, and erases existing copies.	No exceptions noted.
10	There are written procedures describing how the data processor makes available all information necessary in order to demonstrate compliance with the requirements for the processor available to the data controller and allows for and contributes to audits, inspections etc. conducted by the data controller or another auditor mandated by the data controller. A regular – at least annual – assessment is carried out as to whether to update these procedures.	Inspected that there are updated written procedures describing how the data processor makes available to the data controller all information necessary in order to demonstrate compliance with the requirements for the data processor and allows for and contributes to audits, inspections etc. conducted by the data controller or another auditor mandated by the data controller.	No exceptions noted.

Control objective:

Procedures and controls are followed to ensure that the processing of personal data only takes place in accordance with a contract or other legally binding document (data processing agreement) and that data processing is only carried out by data processors approved by the data controller.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
11	A regular – at least annual – assessment is carried out that the data processor has complied with the technical and organisational security measures established so that the data processing fulfils the requirements in the Data Protection Regulation and the Data Protection Act and furthermore ensures protection of the rights of the data subject and that the processing of personal data is performed in accordance with the instructions of the data controller.	Inspected documentation of control describing that the data processor has complied with the technical and organisational security measures established so that the data processing fulfils the requirements in the Data Protection Regulation and the Data Protection Act and furthermore ensures protection of the rights of the data subject and that the processing of personal data is performed in accordance with the instructions of the data controller.	No exceptions noted.
12	Management has dealt with and approved the assessment of compliance with the technical and organisational security measures and data protection and that the processing of personal data has taken place in accordance with instructions from the data controller.	Inspected documentation stating that Management has ensured compliance with the technical and organisational security measures and data protection and that the processing of personal data has taken place in accordance with instructions from the data controller.	No exceptions noted.

Records of processing activities (Article 30)

Control objective:

Procedures and controls are followed to ensure that the processor maintains a record of categories of processing activities conducted on behalf of the data controllers.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	At the data processor, there is a record of categories of processing activities for each data controller that contains: • the name and contact details of the data processor for each data controller and, where applicable, the data controller's data protection officer • the categories of processing carried out on behalf of each data controller • transfers of personal data to a third country or an international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards • a general description of the technical and organisational security measures.	Inspected documentation stating that there is a record of categories of processing activities for each data controller, stating the necessary information.	No exceptions noted.
2	A regular – at least annual – assessment is carried out as to whether the list of categories of processing activities for each data controller should be updated.	Inspected documentation stating that the list of categories of processing activities for each data controller is updated and correct.	No exceptions noted.
3	Management has ensured that the list of categories of processing activities for each data controller is comprehensive, updated and correct.	Inspected documentation stating that Management has ensured that the list of categories of processing activities for each data controller is comprehensive, updated and correct.	No exceptions noted.

Security of processing (Article 32)

Control objective:

Procedures and controls are followed to ensure that, based on a risk assessment, appropriate technical and organisational security measures have been taken against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	The data processor has carried out an independent risk assessment of the processing of personal data for each data controller.	Inspected documentation stating that an independent risk assessment of the processing of personal data for each data controller has been carried out.	No exceptions noted.
2	The data processor has ensured appropriate technical and organisational security measures to ensure a security level appropriate to the risks in the processor's risk assessment.	Inspected documentation stating that appropriate technical and organisational security measures to ensure a security level appropriate to the risks in the data processor's risk assessment have been established. Inspected documentation stating that the established technical and organisational security measures have been efficient during the report period.	No exceptions noted.
3	The technical and organisational security measures established by the data processor are approved by the data controller.	Inspected documentation stating that the data controller has approved the established technical and organisational security measures.	No exceptions noted.
4	A regular – at least annual – assessment is carried out as to whether the risk assessment is up to date and appropriate.	Inspected documentation stating that the data processor's risk assessment is updated and appropriate.	No exceptions noted.
5	A regular – at least annual – assessment is carried out as to whether the technical and organisational security measures cover the risks in the data processor's updated risk assessment.	Inspected documentation stating that the technical and organisational security measures ensure a security level appropriate to the risks in the processor's updated risk assessment.	No exceptions noted.

Control objective:

Procedures and controls are followed to ensure that, based on a risk assessment, appropriate technical and organisational security measures have been taken against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
6	Natural persons at the data processor and sub-processors have been instructed in handling personal data in accordance with the data controller's instructions.	Inspected documentation stating that natural persons at the processor and sub-processors have been instructed in handling personal data in accordance with the data controller's instructions.	No exceptions noted.
7	Management has dealt with and approved the risk assessments.	Inspected documentation stating that Management has dealt with and approved the risk assessments that were valid during the audit period.	No exceptions noted.
8	Management has dealt with and approved the established technical and organisational security measures.	Inspected documentation stating that Management has dealt with and approved the established technical and organisational security measures.	No exceptions noted.

Notification of a personal data breach to the supervisory authority (Articles 33 and 34)

Control objective:

Procedures and controls are followed to ensure that the processor, in the event of a personal data breach, can support the data controller's obligation to satisfactorily notify the supervisory authority in a timely fashion and communicate to the data subjects if personal data are covered by the breach.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	There are written procedures describing the handling of personal data breaches, including communication to the data controller in a timely manner. A regular – at least annual – assessment is carried out as to whether to update these procedures.	Inspected that there are updated written procedures for handling personal data breaches, including a description of communication to the data controller.	No exceptions noted.
2	The data processor ensures the recording of all personal data breaches.	Inspected documentation stating that all personal data breaches are recorded by the data processor.	No exceptions noted.
3	The data processor sends documentation comprising, as a minimum, the facts relating to the breach, its effects and the remedial action taken to the data controller.	Inspected documentation stating that the processor has sent documentation comprising, as a minimum, the facts relating to the breach, its effects and the remedial action taken to the data controller.	No exceptions noted.
4	Management has ensured that personal data breaches are communicated satisfactorily to the data controller in a timely manner.	Inspected documentation stating that Management has ensured that all personal data breaches are communicated satisfactorily to the data controller in a timely manner.	No exceptions noted.

Data protection impact assessment (Article 35)

Control objective:

Procedures and controls are followed to ensure the data processor has received the results of the data controller's impact assessment relating to data protection before the processing of personal data and that a fresh impact assessment is carried out in the event of a change to the risk presented by the processing activities.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	The data processor has received the elements of the results of the data controller's impact assessment for the processing of personal data relevant to the data processor's processing of personal data for each data controller, and the data processor's Management has assessed the need to perform its own impact assessments.	Inspected documentation stating that Management has received relevant results from the data controller's impact assessments. Inspected documentation of Management's assessment of the necessity of performing its own impact assessments on the entire or elements of the data processing for each data controller. No requests have been made in this regard. Procedures and internal controls to handle any requests in this regard are in place in the company.	No exceptions noted.
2	The data processor has established appropriate procedures as well as technical and organisational security measures that ensure processing of personal data in accordance with the data controller's and/or his own impact assessments.	Inspected documentation of the data processor establishing procedures and technical and organisational security measures that ensure processing of personal data in accordance with the data controller's and/or his own impact assessments. No requests have been made in this regard. Procedures and internal controls to handle any requests in this regard are in place in the company.	No exceptions noted.

Control objective:

Procedures and controls are followed to ensure the data processor has received the results of the data controller's impact assessment relating to data protection before the processing of personal data and that a fresh impact assessment is carried out in the event of a change to the risk presented by the processing activities.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
3	The data processor's established procedures as well as technical and organisational security measures for data protection are approved by the data controller before personal data are processed.	Inspected documentation stating that the data processor's established procedures as well as technical and organisational security measures are approved by the data controller. No requests have been made in this regard. Procedures and internal controls to handle any requests in this regard are in place in the company.	No exceptions noted.
4	A regular – at least annual – assessment is carried out as to whether data protection is performed in accordance with the data controller's and/or own impact assessments.	Inspected documentation stating that a regular – at least annual – assessment is carried out as to whether data protection is performed in accordance with the data controller's and/or own impact assessments. No requests have been made in this regard. Procedures and internal controls to handle any requests in this regard are in place in the company.	No exceptions noted.

Prior consultation (Article 36)

Control objective:

Procedures and controls are followed to ensure that the data processor has received the results of the data controller's consultation with the supervisory authority if the impact assessment shows that the processing of personal data will lead to a high risk in the absence of measures taken by the data controller to mitigate the risk.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	The data processor has received the elements of the results from the data controller's consultation with the supervisory authority that is of relevance for the data processor's processing of data for each data controller.	Inspected documentation stating that Management has received the elements of the results from the data controller's consultation with the supervisory authority that is of relevance for the data processor's processing of data for each data controller. No requests have been made in this regard. Procedures and internal controls to handle any requests in this regard are in place in the company.	No exceptions noted.
2	The data processor has established the procedures and the technical and organisational security measures required by the supervisory authority to process the specific personal data.	Inspected documentation stating that requirements from the supervisory authorities have been incorporated into procedures and into technical and organisational security measures. No requests have been made in this regard. Procedures and internal controls to handle any requests in this regard are in place in the company.	No exceptions noted.
3	The data processor's established procedures as well as technical and organisational security measures for ensuring the supervisory authority's requirements are approved by the data controller.	Inspected documentation stating that the data controller has approved the procedures as well as the technical and organisational security measures established by the data processor to ensure the supervisory authority's requirements. No requests have been made in this regard. Procedures and internal controls to handle any requests in this regard are in place in the company.	No exceptions noted.

Control objective:

Procedures and controls are followed to ensure that the data processor has received the results of the data controller's consultation with the supervisory authority if the impact assessment shows that the processing of personal data will lead to a high risk in the absence of measures taken by the data controller to mitigate the risk.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
4	A regular – at least annual – assessment is carried out as to whether data processing is performed in accordance with the supervisory authority's requirements.	Inspected documentation of regular follow-up of compliance with the supervisory authorities' requirements for data processing. No requests have been made in this regard. Procedures and internal controls to handle any requests in this regard are in place in the company.	

Data protection officer (Article 37)

Control objective:

Procedures and controls are followed to ensure that – when required – a data protection officer is appointed who meets the requirements on sufficient expertise and who has been notified to the supervisory authority.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	The data processor has appointed a data protection officer who meets the requirements on sufficient expertise.	The company has not appointed a data protection officer. For this reason, these controls are out of scope.	No exceptions noted.
2	Contact details of the data protection officer have been made public.	The company has not appointed a data protection officer. For this reason, these controls are out of scope.	No exceptions noted.
3	Contact details of the data protection officer have been communicated to the supervisory authority.	The company has not appointed a data protection officer. For this reason, these controls are out of scope.	No exceptions noted.
4	Management has dealt with and approved the appointment of the data protection officer and the assessment of his or her expertise.	The company has not appointed a data protection officer. For this reason, these controls are out of scope.	No exceptions noted.

Position of the data protection officer (Article 38)

Control objective:

Procedures and controls are followed to ensure the data protection officer's position, including that the data protection officer is not instructed on how to perform his or her tasks and does not perform tasks nor has other duties that could lead to a conflict of interest.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	There are written procedures describing the involvement, function and reporting of the data protection officer. A regular – at least annual – assessment is carried out as to whether to update these procedures.	The company has not appointed a data protection officer. For this reason, these controls are out of scope.	No exceptions noted.
2	Management has ensured that it is possible for the data subjects to contact the data protection officer with questions on the processing of their personal data and their rights.	The company has not appointed a data protection officer. For this reason, these controls are out of scope.	No exceptions noted.
3	Management has ensured that the data protection officer is bound by secrecy and confidentiality concerning the performance of his or her tasks.	The company has not appointed a data protection officer. For this reason, these controls are out of scope.	No exceptions noted.
4	Management has ensured that the data protection officer does not perform other task nor has other duties that could lead to a conflict of interest with the data protection officer's tasks and duties.	The company has not appointed a data protection officer. For this reason, these controls are out of scope.	No exceptions noted.

Tasks of the data protection officer (Article 39)

Control objective:

Procedures and controls are followed to ensure that the data protection officer knows the scope of his or her tasks, is sufficiently and timely involved in all matters relating to the protection of personal data and reports directly to the data controller's or the data processor's Management.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	Written procedures for the data protection officer's tasks include: • To inform and advise on obligations pursuant to this regulation etc. • To monitor compliance with this regulation etc. and with the policies of the data processor in relation to the protection of personal data • To provide advise as regards the data protection impact assessment and monitor its performance • To cooperate with the supervisory authority • To act as the contact point for the supervisory authority. A regular – at least annual – assessment is carried out as to whether to update these procedures.	The company has not appointed a data protection officer. For this reason, these controls are out of scope.	No exceptions noted.
2	Management has ensured that the data protection officer has performed his or her tasks in accordance with existing procedures.	The company has not appointed a data protection officer. For this reason, these controls are out of scope.	No exceptions noted.

Transfers of personal data (Articles 44, 45, 46, 47, 48, 49 and 50)

Control objective:

Procedures and controls are followed to ensure that a transfer of personal data to a third country or an international organisation only takes place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection.

No.	Data processor's control activity	Tests performed by PwC	Result of tests performed by PwC
1	There are written procedures that describe the transfer of personal data to a third country or international organisation recognised by the Commission. A regular – at least annual – assessment is carried out as to whether to update these procedures.	There is no transfer of data to third countries as part of delivering the services.	No exceptions noted.
2	There are written procedures describing how appropriate safeguards are provided for the transfer of personal data to a third country or international organisation not recognised by the Commission. A regular – at least annual – assessment is carried out as to whether to update these procedures.	There is no transfer of data to third countries as part of delivering the services.	No exceptions noted.
3	A regular – at least annual – assessment is carried out as to whether third countries or international organisations to which personal data are transferred are still recognised by the Commission.	There is no transfer of data to third countries as part of delivering the services.	No exceptions noted.
4	A regular – at least annual – assessment is carried out as to whether the appropriate safeguards etc. from third countries or international organisations that are *not* recognised and to which personal data are transferred are still sufficient, can be enforced and are effective.	There is no transfer of data to third countries as part of delivering the services.	No exceptions noted.
5	The transfer of personal data to a third country or international organisation – recognised or not recognised by the Commission – is approved by the data controller.	There is no transfer of data to third countries as part of delivering the services.	No exceptions noted.