www.pwc.dk

Assemble

Independent auditor's ISAE 3000 assurance report on internal controls regarding data protection and processing of personal data

April 2020

pwc

Table of content

1. Management statement 4
2. Independent auditor's assurance report 6
3. Assemble's description of setup regarding processing of personal data 8

    Introduction 8

    Description of Assemble's services 8

    General control environment 9

    Risk assessment 10

    Control activities 11

    Information and communication 12

    Monitoring 12

    Complementary controls of data controllers 12

- Report any personal data breaches to the Danish Data Protection Agency. 12

4. Control objectives, controls, tests and related findings 13

    Principles relating to processing of personal data (Article 5) 13

    Lawfulness of processing (Article 6) 14

    Conditions for consent (Articles 7 and 8) 15

    Processing of special categories of personal data (Articles 9 and 10) 16

    Processing that does not require identification (Article 11) 17

    Transparent information, communication and modalities for the exercise of the rights of the data subject (Article 12) 18

    Information to be provided where personal data are collected from the data subject (Articles 13 and 14) 20

    Right of access by the data subject (Article 15) 22

    Right to rectification (Articles 16 and 19) 23

    Right to erasure ('right to be forgotten') (Articles 17 and 19) 24

    Right to restriction of processing (Articles 18 and 19) 25

    Right to data portability (Article 20) 26

    Responsibility of the data controller – implementation of appropriate data protection (Article 24) 27

    Data protection by design and by default (Article 25) 28

    Processor – processing of personal data under the authority of the data controller (Articles 28 and 29) 30

    Records of processing activities (Article 30) 34

    Security of processing (Article 32) 35

    Notification of a personal data breach to the supervisory authority (Articles 33 and 34) 37

    Data protection impact assessment (Article 35) 38

    Prior consultation (Article 36) 39

Data protection officer (Article 37) 40
Position of the data protection officer (Article 38) 41
Tasks of the data protection officer (Article 39) 42
Transfers of personal data (Articles 44, 45, 46, 47, 48, 49 and 50) 43

1. Management statement

Assemble performs processing of personal data on behalf of customers, that are data controllers according to EU's regulation on ”Protection of natural persons with regard to the processing of personal data and on the movement of such data” (subsequently ”Data Protection Regulation”) 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 ”Data Protection Act”).

The accompanying description has been prepared for data controllers, who have used Assemble' services, who have a sufficient understanding to consider the description, along with other information, including information about controls operated by data controller themselves, when assessing whether the requirements in the Data Protection Regulation and Data Protection Act are complied with. Assemble confirms that:

a) The accompanying description in section 2 fairly presents the service handling of personal data on behalf of data controllers regulated by the Data Protection Regulation and Data Protection Act for Assemble customers for the period May 1st 2019 to April 20th 2020. The criteria used in making this statement were that the accompanying description:

   (i) Presents how the system was designed and implemented, including:

   - The types of services provided, including types of personal data processed
   - The procedures, within both information technology and manual systems, by which processing of personal data were initiated, recorded, processed, corrected as necessary, erased and restricted
   - The procedures ensuring that processing of personal data is in accordance with contracts, instructions and agreements with the data controllers
   - The procedures ensuring that the persons authorized to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
   - The procedures for how the 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 law or other regulation requires storage of the personal data
   - The procedures handling of personal data breaches supports that the data controller can communicate to the authorities and inform the data subjects in a timely manner
   - The procedures ensuring adequate technical and organizational measures for the processing of personal data based on the risks associated with the processing for unintentional or illegal erasure, loss, change, unauthorized distribution of or access to personal data, that is transmitted, stored or in any other way processed
   - Controls that we assumed, in the design of the system, would be implemented by data controllers, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by us alone
   - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to processing personal data

   (ii) Includes relevant details of changes to the data processor's system for processing personal data for the period May 1st 2019 to April 20th 2020.

(iii) Does not omit or distort information relevant to the scope of the system being described for 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 system that each individual data controller may consider important in its own particular environment.

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively for the period May 1st 2019 to April 20th 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 individuals who have the appropriate competence and authority, for the period May 1st 2019 to April 20th 2020

b) Appropriate technical and organizational security measures has been implemented and maintained to comply with the agreements with the data controllers, good practice for data processing and relevant requirements for data processors according to the Data Protection Regulation and Data Protection Act.

Hellerup April 21 2020

Assemble A/S
Morten Svendsen
CEO

2. Independent auditor's assurance report

Independent auditor's ISAE 3000 assurance report on internal controls regarding data protection and processing of personal data

To the Management of Assemble, Assembles customers as data controllers

Scope
We have been engaged to report on Assembles description in section 3 on processing of personal data on behalf of customers who are data controllers according to EU's regulation on the "Protection of natural persons with regard to the processing of personal data and on the movement of such data" (subsequently the "Data Protection Regulation") 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 Act") for the period May 1st 2019 to April 20th 2020 (the description) and the design and operation of controls related to the control objectives stated in the description.

We express reasonable assurance in our conclusion.

Our report covers whether Assemble as a Service has established and designed appropriate controls related to the control objectives stated in section 4 regarding Assemble as a Service's role as a data processor. Thus, the report does not include an assessment of Assemble as a Service's general compliance with the above legislation.

Assembles responsibilities
Assemble is responsible for: preparing the description and accompanying statement in section 1, including for 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, implementing and effectively operating controls to achieve the stated control objectives.

Our 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 is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

PricewaterhouseCoopers applies International Standard on Quality Control 1 and accordingly 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.

Service auditor's responsibilities
Our responsibility is to express an opinion on Assembles description and on the design and operation of controls related to the control objectives stated in the description, based on our procedures.

We have conducted our assurance engagement in accordance with International Standard on Assurance Engagements 3000, "Assurance engagements other than audits or reviews of historical financial information" and other requirements according to Danish audit regulation. This standard requires that we plan and perform our work 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 system and the design and operating effectiveness of controls. The procedures selected depend on the service 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 considered 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 section 3.

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
Assembles description has been prepared to meet the common needs of a data controller and may not, therefore, include every aspect of data processing that every single data controller may consider important in its own particular environment. Also, because of their nature, controls at a data processor may not prevent or detect all breaches of personal data. Furthermore, the projection of any evaluation of 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 report. The criteria we used in forming our opinion are those described in section 3. In our opinion, in all material aspects:

a) The description fairly presents the operational services as designed for the period May 1st 2019 to April 20th 2020

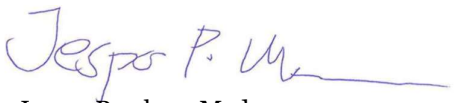
b) The controls related to the control objectives stated in the description were suitably designed for the period May 1st 2019 to April 20th 2020

c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives were achieved, operated effectively for the period May 1st 2019 to April 20th 2020.

Description of tests of controls
The specific controls tested and the nature, timing and results of these 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 Assembles data processing of personal data and who have a sufficient understanding to consider these, along with other information, including information about controls operated by data controllers themselves, when assessing whether the requirements in the Data Protection Regulation has been complied with.

Aarhus, 21 April 2020
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab



Jesper Parsberg Madsen
State-Authorised Public Accountant

3. Assemble's description of setup regarding processing of personal data

Introduction

Assemble develops, implements and maintains management, collaboration, and documentation solutions for daycare centers, schools, colleges and the health sector. All solutions have a high focus on easy management and implementation, user friendly use and integration with other platforms in a secure manner.

Description of Assemble's services

This independent auditor's assurance report focuses on the solutions developed for colleges, schools and daycare centers: Nembørn, Nemplads, Nemindsigt, Nempost, Assemble LMS and Assemble Heart.

Assembles solutions are currently hosted by private cloud with Itadel in Denmark and public cloud in Microsoft Azure. The activities with Microsoft Azure and Itadel are not part of this declaration.

Assembles solutions have been deployed in over 20 Danish municipalities and over 6.000 institutions across 4 continents.

Nembørn

Nembørn is the digital solution from Assemble for schools and daycare centers. Designed from the ground up with an inclusive mindset, Assemble has created a solution to foster creativity, collaboration and communication for children, students, parents and teachers.

With a view of the child from birth to graduation, Assemble can facilitate the learning process in a holistic way. Nembørn connects parents and teachers through extensive documentation to create a better learning environment for children and students.

By communicating and documenting throughout the school-day, children's learning can continuously be extended to the home. Parents can also rest assured that their children's wellbeing are being documented and accounted for.

Nembørn creates a safe and inclusive learning environment in the child's school and home.

Nemplads

Nemplads is a modern capacity- and resource-management platform from Assemble. Developed for municipalities, schools and daycare centers to ease the administrative workloads by transforming the way they can manage and run their institutions.

Nemplads provides a new user-friendly capacity-management system for parents and employees to use for management of available spots in the institution, economic benefits, invoicing and finance.

Nemplads includes a self-service tool for parents to manage their children's enrolments, book spots in available daycare centers or schools and report state-funded benefits in an easy and intuitive way.

Nemindsigt

Assemble has built a user-friendly and secure self-service tool for citizen and authorities for increased transparency and accountability in public case processing. Nemindsigt, Nemsag and Nemvalider provides an intuitive access for case management and documentation for journaling and processing purposes in a secure manner.

Nempost

Nempost is an easy and secure email platform for encrypted and digitally signed dialog between citizens and authorities. Nempost and Nemsend enables the users to send secure email with the same validity as a traditional hand-signed letter and the platform automates all processes regarding sending and receiving mail.

Assemble LMS

As an extension of Nembørn, Assemble LMS is a solution for learning and development management in colleges and higher education institutions.

Assemble LMS is used by students and teachers during their daily education to view and progress through course curriculum. With Assemble LMS teachers have the ability to build their own course curriculum for entire classes and have enough flexibility to tailor courses to individual participants.

Assemble LMS enables a differentiated and individualistic educational experience for students and course participants.

The platform supports different test mechanisms, various assessments based on progression and participation and includes assignment hand-ins. Courses and assessments can be differentiated to the individual participants for various delivery mechanisms, whether online, at the institution or participants with reading disabilities.

Assemble Heart

Assemble has developed a new solution to measure heart rhythm, EKG, pulse etc. for patients.

Assemble Heart provides a possibility for increased communication and sharing between patients and health professionals for monitoring purposes to increase the possible detection of heart attacks.

Assemble Heart utilizes the newest health technologies including smart wearables with support for EKG measurement.

General control environment

The responsibility for continuously ensuring the protection of personal data within Assemble lies with the security group and is comprised of

- Morten Svendsen, CEO
- Jesper Broe Rasmussen, Data Compliance Officer
- Elsebeth Svendsen, CFO and legal compliance

The work of the security group is planned in a GDPR year plan comprising relevant activities to ensure that Assemble is always compliant according to applicable law.

Different members of the security group meet every month according to the year plan and reviews the current data protection level, including a discussion of IT security initiatives to increase the IT security level.

The perspective and agenda vary from month to month according to the different activities in the year plan, and during the calendar year, the following areas are discussed one or more times:

- IT security policy (always updated)
- Review of data protection policy, including procedures and guidelines
- Review of security
- Review of any security breaches
- Procedures for access to personal data
- Procedures for risk assessment
- Procedures for security related to support
- Follow up on training and awareness

As regards concluded data processing agreements:

- Follow-up on receipt of (new) data processing agreements and approval of them
- Follow-up on customers with special requirements in their data processing agreements
- Follow-up on approval of potential sub-suppliers
- Follow-up to verify that the data controller has approved any procedures and technical measures that ensure the processing and protection of personal data
- Follow-up to verify that any sub-data processors has implemented procedures and technical measures that ensure the processing and protection of personal data
- Follow-up to verify that enquiries from the data controller with regard to the rights of data subjects (access, erasure, rectification) have been handled in an appropriate and timely manner.
- Follow-up to verify that enquiries from the data controller with regard to Security of processing (Article 32), Notification of a personal data breach to the supervisory authority (Article 33), Communication of a personal data breach to the data subject (Article 34), Data protection impact assessment (Article 35) and Prior consultation (Article 36) have been handled in an appropriate and timely manner.

As regards any incidents occurred:

- Follow-up on the result of the data controller's consultation of the supervisory authority to the extent this is relevant to Assemble's processing of data for this data controller.
- Follow-up to verify that individuals authorised to process personal data are bound to confidentiality or are under a statutory obligation of confidentiality

Assemble has appointed Jesper Broe Rasmussen as a Data Compliance Officer with the responsibility to ensure the processes and services of Assemble complies with GDPR.

The IT Security Policy and Data Protection Policy (customer-facing) of Assemble apply to all the employees of Assemble and are part of the basis of the employment relationship. The policies provide the framework for the processing, storage, sharing and erasure of data, and they contain procedures for rights management, password management, patching, logging, backup, access control, etc.

The policies are updated at specified intervals and, as a minimum, when the company introduces new systems, services, business processes etc. of importance to the security or data protection.

All documents relating to data protection, including documentation, risk analyses, policies, reports, etc., are stored in document archive. Access to these resources are restricted so that only relevant employees have access to the various information about the handling and follow-up on the data controller's enquiries/requests for support, e.g. support for responding to a request from a data subject (the end user) regarding his/her rights, as well as the data controller's enquiries regarding Assemble assessment and consultation with the supervisory authority. Likewise, only members of the security group have access to the documentation/analysis in the event of a security breach. No personal sensitive information is stored in the document archive. Personal sensitive information is only stored in system, where access is secured by 2-factor authentication.

The various policies and process descriptions are available to all employees on the company Intranet.

The security group is responsible for checking that the required controls are carried out and have the intended effect. The results are discussed in the security group, and any necessary actions are agreed.

Risk assessment

Assemble has formalised processes for assessing the risk of the services in which personal data are processed.

The risk assessment is reviewed at specified intervals and, additionally, as a minimum when a system is modified, new business processes are implemented, a new system is applied or when we process new types of personal data as part of our services.

The focal point of the risk assessments is the risk/likelihood of a personal data breach and the consequences to the data subject of such a breach.

The risk assessments help ensure that the necessary technical and organisational security measures are always set up to protect the data being processed either in the solutions or in the organisation. The risk assessment is used in the continued effort to establish organisational and technical security measures to counter the risks (risk management) stated in the risk assessment.

Risk assessments are made by the Data Compliance Officer with input from relevant employees in the development department of the organisation. Risk assessments are approved by the security group.

The current risk landscape

Considering the data we process – together with the controls and the organisational and technical measures we have implemented to mitigate risk and minimise the likelihood of personal data breaches – the current risk profile of Assemble's services is assessed as being low. To ensure a constant focus on minimising our risks, we have established control activities aiming at both safeguarding and testing that our measures adequately mitigate these risks.

Control activities

Assemble has formal processes that ensure that the security of personal data is considered when onboarding new customers. Thus, prior to deployment/launch of a new project, we e.g. check that our customers are familiar with our procedures and ways of working and that we live up to our responsibilities for good data processing practice as well as to our obligations as a data processor for our customers.

Assemble has formal procedures that ensure that data are not stored locally and that data are deleted in our systems in due course after processing. Furthermore, employees at Assemble are committed to observing and ensuring that our data deletion policy is followed.

Assemble inspects all (sub-)processors once a year and if the nature of the cooperation changes. The inspection is made on the basis of relevance and risk. This means that the nature, scope, relation and purpose of the processing in question, as well as the risk to the rights and freedoms of individuals, are taken into consideration. The greater the risk, the greater the requirements for security. The inspection is made by obtaining assurance reports and gathering written information. Depending on the risk related to the sub-processor's processing activities, the gathering of written information may be complemented by physical visits.

(Sub-)processing agreements are entered with all (sub-)processors in which the sub-processors have at least the same obligations as Assemble does towards the customer.

Inspection is carried out to verify that the concluded (sub-)processing agreement is observed, including that the (sub-)processor has implemented the agreed technical and organisational security measures.

Assemble has established a compliance set-up composed of controls that are carried out internally in the organisation at the agreed frequency in accordance with the purpose of the procedure. These controls have been established to ensure compliance with the above initiatives and procedures as well as with other GDPR matters. The controls are system-controlled to allow us to ensure follow-up and escalation in case of lack of execution. The security group at Assemble has the primary responsibility for operating and managing this control set-up although the execution of the controls may be delegated to the relevant people in a certain area of responsibility.

Information and communication

When onboarding new employees at Assemble, they receive relevant information and awareness in handling personal data and in Assemble's processes for protecting personal data.

Assemble handles all communications with data subjects through formal processes supported by the hotline and Task management systems used in Assemble.

Monitoring

Following a formal procedure, the security board follow up on a quarterly basis the status on the GDPR work, the receipt and approval of (new) data processing agreements and follow-up to verify that the enquiries from the data controller with regard to the rights of data subjects (access, erasure, rectification) have been handled in an appropriate and timely manner.

Complementary controls of data controllers

As part of the delivery of services, the data controller must implement certain controls that are important to achieve the control objectives specified in the description. This includes:

- Consider the consequences related to the protection of personal data when change requests are raised
- Be responsible for ensuring that a legal basis for processing exists at the time of the transfer of the personal data to Assemble – 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 Assemble 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, controls, tests and related findings

Principles relating to processing of personal data (Article 5)

Control objective:

Procedures and controls have been established 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.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
1	There are written procedures in which a decision has been made on the following principles related to 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 to check whether the procedures need to be updated.	Inspected that there are updated written procedures for processing of personal data that include principles related to processing of personal data.	No exceptions noted.
2	There are regular – at least annual – assessments that principles related to processing of personal data are being complied with, and this assessment is documented.	Inspected documentation for the assessment of principles related to processing of personal data in order to ensure that an annual assessment is carried out at least annually of principles for processing of personal data and compliance with these.	No exceptions noted.
3	Management has dealt with and approved the assessment of compliance with the principles related to 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 established to ensure that personal data are only processed lawfully.

No.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
1	There are written procedures that contain requirements that personal data must only be processed where there is a lawful basis. Regular – at least annual – assessments are carried out to check whether the procedures need to be updated.	Inspected that there are updated written procedures for processing of personal data that contain requirements for the lawful processing of personal data.	No exceptions noted.
2	There is a data processor agreement or suchlike approved by the data controller and containing a summary of the basis on which processing of personal data is carried out.	Inspected documentation of the basis on which processing of personal data is carried out and that this is approved by the data controller (data processor agreement etc.).	No exceptions noted.
3	An update is carried out regularly – at least annually – of the statement by the data controller of the basis on which the processing of personal data is carried out.	Inspected documentation 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	There is a regular – at least annual – assessment 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 have been established to ensure that data subjects have provided written consent to the processing of personal data.

No.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
1	There are written procedures for acquiring written consent to processing of personal data. Regular – at least annual – assessments are carried out to check whether the procedures need to be updated.	Inspected that there is an updated written procedure for obtaining written consent to processing of personal data.	Not relevant for the services in scope.
2	A regular – at least annual – control is carried out that written consent to the processing of personal data has been obtained.	Inspected documentation that a control has been carried out that written consent to the processing of personal data has been obtained.	Not relevant for the services in scope.
3	Management has dealt with and approved the control that written consent to the processing of personal data has been obtained.	Inspected documentation of Management's approval of the assessment of obtaining written consent to the processing of personal data.	Not relevant for the services in scope.

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

Control objective:

Procedures and controls are established 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.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
1	Written procedures exist in which it is decided that the processing of special categories of personal data must only take place at the processor if the criteria for processing is specifically agreed with the individual data controller. Regular – at least annual – assessments are carried out to check whether the procedures need to be updated.	Inspected that updated written procedures exist where it is decided that the processing of special categories of personal data at the processor must only take place if the criteria for processing are specifically agreed with the data controller.	No exceptions noted.
2	There is a data processor 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 that the processing of special categories of personal data is carried out on the basis approved by the data controller.	No exceptions noted.
3	There is a regular – at least annual – assessment of 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 that does not require identification (Article 11)

Control objective:

Procedures and controls have been established to ensure that the maintaining, acquiring and processing of information for the identification of the data subject are adhered to as long as identification is required.

No.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
1	There are written procedures that ensure that the maintaining, acquiring and processing of information for the identification of the data subject are adhered to as long as identification is required. Regular – at least annual – assessments are carried out to check whether the procedures need to be updated.	Inspected that there are updated written procedures that ensure that the maintaining, acquiring and processing of information for the identification of the data subject are adhered to as long as identification is required.	No exceptions noted.
2	There is a statement of criteria for the maintaining, acquiring and processing of information for the identification of the data subject that has been approved by the data controller.	Inspected documentation that criteria for the maintaining, acquiring and processing of information for the identification of the data subject have been approved by the data controller.	No exceptions noted.
3	There is a regular – at least annual – update of the list of criteria approved by the data controller for the maintaining, acquiring and processing of information for the identification of the data subject.	Inspected documentation that there is a regular – at least annual – update of the list of criteria approved by the data controller for the maintaining, acquiring and processing of information for the identification of the data subject.	No exceptions noted.
4	There is a regular – at least annual – assessment that the maintaining, acquiring and processing of information for the identification of the data subject take place in accordance with the criteria from the data controller.	Inspected documentation that the maintaining, acquiring and processing of information for the identification of the data subject take place in accordance with the criteria from the data controller.	No exceptions noted.
5	Management has dealt with and approved the assessment of whether the maintaining, acquiring and processing of information for the identification of the data subject take place in accordance with the criteria from the data controller.	Inspected documentation of Management's approval of the assessment that the maintaining, acquiring and processing of information for the identification of the data subject take place as long as this is required in accordance with 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 have been established to ensure that information to the data subject about the processing of personal data can be provided in a transparent, intelligible and easily accessible form.

No.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
1	There are written procedures describing how it is ensured that information about the processing of personal data can be provided to the data subject or how the processor can assist the data controller with this. Regular – at least annual – assessments are carried out to check whether the procedures need to be updated.	Inspected that there are updated written procedures describing how it is ensured that information about the processing of personal data can be provided to the data subject or the data controller.	Not relevant for the services in scope.
2	There is an updated description of information about the processing of personal data, which is approved by the data controller.	Inspected the description of information about the processing of personal data to ensure that the information will be shown in a transparent, intelligible and easily accessible form to the data subject. Inspected that the description of information about the processing of personal data is updated and approved by the data controller.	Not relevant for the services in scope.
3	Management has ensured that information about the processing of personal data is updated and approved by the data controller.	Inspected documentation that Management has ensured that information about the processing of personal data is updated and approved by the data controller.	Not relevant for the services in scope.
4	There are written procedures describing how it is ensured that the data subject's requests and motivation of any refusals are responded to in a timely manner, or how the processor can assist the data controller with this. Regular – at least annual – assessments are carried out to check whether the procedures need to be updated.	Inspected that there are updated written procedures describing how it is ensured that the data subject's requests and motivation of any refusals are responded to in a timely manner.	Not relevant for the services in scope.

Control objective:

Procedures and controls have been established to ensure that information to the data subject about the processing of personal data can be provided in a transparent, intelligible and easily accessible form.

No.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
5	It is regularly – and at least annually – ensured that responses to requests from data subjects are provided in a timely manner.	Inspected documentation that actual responses to requests from data subjects are provided in a timely manner and in accordance with procedures.	Not relevant for the services in scope.
6	Management has ensured that the data subject's requests and motivation of any refusals are handled correctly and in a timely manner.	Inspected documentation that Management has ensured that the responses are handled correctly and in a timely manner.	Not relevant for the services in scope.

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

Control objective:

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

No.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
1	There are written procedures describing how it is ensured that the data subject receives information about 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 processor can assist the data controller with this. Regular – at least annual – assessments are carried out to check whether the procedures need to be updated.	Inspected that there are updated written procedures describing how it is ensured that the data subject receives information about the purpose of processing the personal data and information on any transfer of personal data to recipients, third countries or international organisations.	Not relevant for the services in scope.
2	There is an updated description of information about the processor's processing of personal data etc., which is approved by the data controller.	Inspected documentation that the description of information about the processing of personal data etc. is updated and approved by the data controller.	Not relevant for the services in scope.
3	Management has ensured that information about the processor's processing of personal data etc. is updated and approved by the data controller.	Inspected documentation that Management has ensured that the description is updated and approved by the data controller.	Not relevant for the services in scope.
4	There are written procedures describing the provision of information about the right to access to, rectification or erasure of personal data and restriction of processing, or how the processor can assist the data controller with this. Regular – at least annual – assessments are carried out to check whether the procedures need to be updated.	Inspected that there are written procedures describing the provision of information about the right to access to, rectification or erasure of personal data and restriction of processing.	Not relevant for the services in scope.
5	There is an updated description of the data subject's right to access to, rectification or erasure of personal data, which has been approved by the data controller.	Inspected documentation that there is an updated description of the data subject's right	Not relevant for the services in scope.

Control objective:

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

No.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
		to access to, rectification or erasure of personal data, which has been approved by the data controller.	
6	There is a regular – at least annual – control that all data subjects have received the description of the data subject's right to access to, rectification or erasure of personal data.	Inspected documentation of control that all data subjects have received the description of the data subject's right to access to, rectification or erasure of personal data.	Not relevant for the services in scope.
7	Management has ensured that the description of the data subject's right to access, rectification etc. is updated and approved by the data controller and communicated to all the data subjects.	Inspected documentation that management has ensured that the description of the data subject's right to access, rectification etc. is updated and approved by the data controller and all data subjects have received the description.	Not relevant for the services in scope.

Right of access by the data subject (Article 15)

Control objective:

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

No.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
1	There are written procedures describing how data subjects' requests to access their own registered personal data are handled, or how the processor can assist the data controller with this. Regular – at least annual – assessments are carried out to check whether the procedures need to be updated.	Inspected that there are written procedures describing how data subjects' requests to access their own registered personal data are handled.	Not relevant for the services in scope.
2	The processor has a description for the data subject of how personal data are collected, processed and stored, which is approved by the data controller.	Inspected documentation that the description of information about the processing of personal data etc. is approved by the data controller.	Not relevant for the services in scope.
3	The 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 that the content of the extraction of personal data is approved by the data controller.	Not relevant for the services in scope.
4	There is a regular – at least annual – assessment of whether the extraction of personal data to the data subject and description of how the personal data will be processed is updated and correct.	Inspected documentation that the extraction of personal data to the data subject and description of how the personal data will be processed is updated and correct.	Not relevant for the services in scope.
5	It is regularly – and at least annually – ensured that responses to requests from data subjects are provided in a timely manner.	Inspected documentation that actual responses to requests from data subjects are provided in a timely manner and in accordance with procedures.	Not relevant for the services in scope.
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 that 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.	Not relevant for the services in scope.

Right to rectification (Articles 16 and 19)

Control objective:

Procedures and controls have been established 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.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
1	There are written procedures describing the handling of data subjects' right to rectification of personal data, or how the processor can assist the data controller with this. Regular – at least annual – assessments are carried out to check whether the procedures need to be updated.	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 that technical measures have been established in the IT systems used in order to rectify personal data. Inspected documentation that personal data are only rectified by means of the established technical measures.	No exceptions noted.
3	There is a regular – at least annual – assessment that the rectification of personal data takes place correctly and without undue delay.	Inspected documentation 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 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 have been established 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.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
1	There are written procedures describing the handling of data subjects' right to erasure of personal data, or how the processor can assist the data controller with this. Regular – at least annual – assessments are carried out to check whether the procedures need to be updated.	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 that technical measures have been established in the IT systems used in order to erase personal data. Inspected documentation that personal data are only erased by means of the established technical measures.	No exceptions noted.
3	There is a regular – at least annual – assessment that the erasure of personal data takes place correctly and without undue delay.	Inspected documentation 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 that the erasure of personal data has taken place correctly and without undue delay.	Inspected documentation 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 have been established to ensure that the data subject's right to restriction of processing of his own registered personal data is complied with, including restriction of processing at recipients of the personal data.

No.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
1	There are written procedures describing the handling of data subjects' right to restriction of processing of personal data, or how the processor can assist the data controller with this. Regular – at least annual – assessments are carried out to check whether the procedures need to be updated.	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 processing of personal data can be restricted.	Inspected documentation that technical measures have been established in the IT systems used in order to restrict the processing of personal data. Inspected documentation that personal data are only restricted by means of the established technical measures.	No exceptions noted.
3	There is a regular – at least annual – assessment that the restriction of processing of personal data takes place correctly and without undue delay.	Inspected documentation that the restriction of processing 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 restriction of personal data has taken place correctly and without undue delay.	Inspected documentation that Management has ensured that the restriction of 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 have been established to ensure that the data subject's right to transfer his own registered personal data to another data controller is complied with.

No.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
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. Regular – at least annual – assessments are carried out to check whether the procedures need to be updated.	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 that technical measures have been established in the IT systems used to ensure it is possible to transfer personal data. Inspected documentation that the transfer of personal data only takes place by means of the technical measures.	No exceptions noted.
3	The 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 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 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 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 have been established 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.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
1	The processor has received instructions for the processing and protection of personal data from the data controller.	Inspected documentation that the data controller has given the 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 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 controller has a description of the use of other processors, including a description of the other processors' 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 that the data controller has approved the processor's other 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 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 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 have been established to ensure that the requirements for data protection by design and by default in the processor's technical and organisational security measures function effectively.

No.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
1	There are written procedures describing data protection by design and by default, including how the processor can assist the data controller in the safeguarding of this. Regular – at least annual – assessments are carried out to check whether the procedures need to be updated.	Inspected that there are updated written procedures describing data protection by design and by default, including how the 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 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 that the established technical and organisational security measures have functioned effectively during the statement period.	No exceptions noted.
3	The technical and organisational security measures established by the processor are approved by the data controller.	Inspected documentation 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 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 processor has received instructions from the data controller regarding which personal data are necessary (data minimisation) and how these shall be processed in relation to the individual specific purpose of processing.	Inspected documentation of the data controller's instructions to the processor regarding which personal data are necessary and how	No exceptions noted.

Control objective:

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

No.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
		these shall be processed in relation to the specific purpose of processing.	
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, the processing of personal data has taken place in accordance with requirements and instructions from the data controller and the approved procedures.	Inspected documentation that Management has ensured that the technical and organisational security measures and data protection and processing of personal data have taken place in accordance with the requirements and instructions from the data controller and the approved procedures.	No exceptions noted.

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

Control objective:

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

No.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
1	A contract or other legally binding document (data processor agreement) has been entered into between processor and data controller that describes the technical and organisational security measures that the processor has established so that the data processing fulfils the requirements in the Data Protection Regulation and Data Protection Act and ensures protection of the rights of the data subject.	Inspected documentation that the data processor agreement describes the technical and organisational security measures that the processor has established so that the data processing fulfils the requirements in the Data Protection Regulation and Data Protection Act and ensures protection of the rights of the data subject.	No exceptions noted.
2	The processor has received – specific or general – authorisation from the data controller to use other processors. Where there is a written general authorisation, the processor shall inform the data controller of any intended changes concerning the addition or replacement of other processors.	Inspected documentation that the data controller has authorised the use of other processors. Inspected documentation that intended changes concerning the addition or replacement of other processors have taken place following notification to the data controller.	No exceptions noted.
3	The processor has received the data controller's instructions for the processing and protection of personal data from the data controller.	Inspected documentation that the data controller has given the processor instructions on the processing and protection of personal data.	No exceptions noted.
4	There are written procedures describing that only the 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 of whether the procedures need to be updated.	Inspected that there are updated written procedures that only the 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:

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

No.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
5	There are written procedures describing that the processor will ensure that the persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. A regular – at least annual – assessment is carried out to check whether the procedures need to be updated.	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 confidentiality.	No exceptions noted.
6	There are written procedures that – where the processor uses other processors to perform specific processing activities on behalf of the data controller – describe the processor's controls to ensure that the other processor complies with the same data protection obligations as set out in the data processor contract between the data controller and the processor. A regular – at least annual – assessment is carried out to check whether the procedures need to be updated.	Inspected that there are written procedures that describe the processor's controls to ensure that the other processor complies with the same data protection obligations as set out in the data processor contract between the data controller and the processor.	No exceptions noted.
7	There are written procedures describing how the 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 to check whether the procedures need to be updated.	Inspected that there are updated written procedures describing how the processor assists the data controller 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.	No exceptions noted.
8	There are written procedures describing how the data subject –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 processor assists the data controller with ensuring compliance with the data controller's obligations.	No exceptions noted.

Control objective:

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

No.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
	• 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 to check whether the procedures need to be updated.		
9	There are written procedures describing how the 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 to check whether the procedures need to be updated.	Inspected that there are updated written procedures describing how the 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 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 to check whether the procedures need to be updated.	Inspected that there are updated written procedures describing how the processor makes available to the data controller all information necessary in order to demonstrate compliance with the requirements for the 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.
11	There is a regular – at least annual –assessment that the processor and data controller has complied with the technical and organisational security measures established so that the data processing fulfils the requirements in the Data Protection Regulation and Data Protection Act and ensures protection of the rights of the data subject and	Inspected documentation for control 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 Data Protection Act and ensures protection of the rights of the data subject	No exceptions noted.

Control objective:

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

No.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
	that processing of personal data takes place in accordance with the data controller's instructions.	and that processing of personal data takes place in accordance with the data controller's instructions.	
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 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 have been established to ensure that the processor maintains a record of categories of processing activities conducted on behalf of the data controllers.

No.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
1	At the processor, there is a record of categories of processing activities for each data controller, which contains: • the name and contact details of the 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 that there is a record of categories of processing activities for each data controller, stating the necessary information.	No exceptions noted.
2	There is a regular – at least annual – assessment of whether the list of categories of processing activities for each data controller should be updated.	Inspected documentation 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 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 have been established 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.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
1	The processor has carried out an independent risk assessment of the processing of personal data for each data controller.	Inspected documentation that an independent risk assessment of the processing of personal data for each data controller has been carried out.	No exceptions noted.
2	The 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 that appropriate technical and organisational security measures to ensure a security level appropriate to the risks in the processor's risk assessment have been established. Inspected documentation that the established technical and organisational security measures have functioned effectively during the statement period.	No exceptions noted.
3	The technical and organisational security measures established by the processor are approved by the data controller.	Inspected documentation 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 to check whether the risk assessment is updated and appropriate.	Inspected documentation that the processor's risk assessment is updated and appropriate.	No exceptions noted.
5	There is a regular – at least annual – assessment of whether the technical and organisational security measures cover the risks in the processor's updated risk assessment.	Inspected documentation 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.
6	Natural persons at the processor and other processors have been instructed in handling personal data in accordance with the data controller's instructions.	Inspected documentation that natural persons at the processor and other processors have been instructed in handling personal data in accordance with the data controller's instructions.	No exceptions noted.

Control objective:

Procedures and controls have been established 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.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
7	Management has dealt with and approved the risk assessments.	Inspected documentation 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 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 have been established 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.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
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 to check whether the procedures need to be updated.	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 processor ensures the recording of all personal data breaches.	Inspected documentation that all personal data breaches are recorded by the processor.	No exceptions noted.
3	The 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 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 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 have been established to ensure the processor has received the results of the data controller's impact assessment relating to data protection before 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.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
1	The processor has received the element of the results of the data controller's impact assessment for the processing of personal data relevant to the processor's processing of personal data for each data controller and the processor's Management has assessed the need to perform its own impact assessments.	Inspected documentation 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 exceptions noted.
2	The processor has established appropriate procedures, technical and organisational security measures that ensure processing of personal data in accordance with the data controllers' and/or his own impact assessments.	Inspected documentation of the processor establishing procedures and technical and organisational security measures that ensure processing of personal data in accordance with the data controllers' and/or his own impact assessments.	No exceptions noted.
3	The processor's established procedures, technical and organisational security measures for data protection are approved by the data controller before personal data are processed.	Inspected documentation that the processor's established procedures, technical and organisational security measures are approved by the data controller.	No exceptions noted.
4	There is a regular – at least annual – assessment of whether data protection is performed in accordance with the data controllers' and/or own impact assessments.	Inspected documentation that there is a regular – at least annual – assessment of whether data protection is performed in accordance with the data controllers' and/or own impact assessments.	No exceptions noted.

Prior consultation (Article 36)

Control objective:

Procedures and controls have been established to ensure that the 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.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
1	The processor has received the elements of the results from the data controller's consultation with the supervisory authority that are of relevance for the data controllers processing of data for each data controller.	Inspected documentation that Management has received the elements of the results from the data controller's consultation with the supervisory authority that are of relevance for the data controllers processing of data for each data controller.	No exceptions noted.
2	The processor has established the procedures, technical and organisational security measures required by the supervisory authority to process the specific personal data.	Inspected documentation that requirements from the supervisory authority have been incorporated into procedures, technical and organisational security measures.	No exceptions noted.
3	The processor's established procedures, technical and organisational security measures for ensuring the supervisory authority's requirements are approved by the data controller.	Inspected documentation that the data controller has approved the procedures, technical and organisational security measures established by the processor to ensure the supervisory authority's requirements.	No exceptions noted.
4	There is a regular – at least annual – assessment of whether data processing is performed in accordance with the supervisory authority's requirements.	Inspected documentation of regular follow-up of compliance with the supervisory authority's requirements for data processing.	No exceptions noted.

Data protection officer (Article 37)

Control objective:

Procedures and controls have been established to ensure – in those cases where this is necessary – that a data protection officer has been designated who fulfils the requirements for sufficient competence and who has been notified to the supervisory authority.

No.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
1	The processor has designated a data protection officer who complies with the requirements for sufficient competence.	Inspected documentation of the processor's assessment of whether the designated data protection officer has the necessary competences.	Not relevant for the services in scope.
2	Contact details for the data protection officer have been published.	Inspected documentation that contact details for the data protection officer have been published.	Not relevant for the services in scope.
3	Contact details for the data protection officer have been notified to the supervisory authority.	Inspected documentation that contact details for the data protection officer have been notified to the supervisory authority.	Not relevant for the services in scope.
4	Management has dealt with and approved the designation of the data protection officer and the assessment of his competences.	Inspected documentation that Management has dealt with and approved the designation of the data protection officer, including ensuring the data protection officer's competences.	Not relevant for the services in scope.

Position of the data protection officer (Article 38)

Control objective:

Procedures and controls have been established to ensure the position of the data protection officer, including a data protection officer not receiving instructions regarding the exercise of his tasks and a data protection officer not performing tasks or having other duties that could lead to a conflict of interests.

No.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
1	Written procedures have been prepared that describe the involvement, effect and reporting of the data protection officer. A regular – at least annual – assessment is carried out to check whether the procedures need to be updated.	Inspected that there are updated written procedures for the involvement, effect and reporting of the data protection officer to ensure that this is satisfactory and updated.	Not relevant for the services in scope.
2	Management has ensured that it is possible for data subjects to contact the data protection officer regarding questions concerning the processing of their personal data and their rights.	Inspected documentation that data subjects have the opportunity to contact the data protection officer.	Not relevant for the services in scope.
3	Management has ensured that the data protection officer is bound by secrecy and confidentiality concerning the performance of his tasks.	Inspected documentation that Management has bound the data protection officer to secrecy and requirements for confidentiality.	Not relevant for the services in scope.
4	Management has ensured that the data protection officer does not perform other tasks or have other duties that could lead to a conflict of interest with the data protection officer's tasks and duties.	Inspected documentation that Management has ensured that the data protection officer does not perform other tasks or have other duties that could lead to a conflict of interest with the data protection officer's tasks and duties.	Not relevant for the services in scope.

Tasks of the data protection officer (Article 39)

Control objective:

Procedures and controls have been established to ensure that the data protection officer is aware of the scope of his tasks, is sufficiently involved in a timely manner in all questions concerned with the protection of personal data and reports directly to the data controller or processor's Management.

No.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
1	Written procedures for the data protection officer's tasks include: • Informing and advising of obligations pursuant to this Regulation etc. • Monitoring compliance with this Regulation etc. and with the policies of the data controller in relation to the protection of personal data • Providing advice as regards the data protection impact assessment and monitoring its performance • Cooperating with the supervisory authority • Acting as the contact point for the supervisory authority. A regular – at least annual – assessment is carried out to check whether the procedures need to be updated.	Inspected that there are updated written procedures for the data protection officer's tasks to ensure that these are satisfactory and updated.	Not relevant for the services in scope.
2	Management has ensured that the data protection officer has performed his tasks in accordance with the existing procedures.	Inspected documentation that Management has ensured that the data protection officer has performed his tasks in accordance with the existing procedures.	Not relevant for the services in scope.

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

Control objective:

Procedures and controls have been established 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.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
1	There are written procedures describing 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 to check whether the procedures need to be updated.	Inspected that there are updated procedures describing the transfer of personal data to a third country or international organisation recognised by the Commission to ensure that these are satisfactory.	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 to check whether the procedures need to be updated.	Inspected that there are updated procedures describing the transfer of personal data to a third country or international organisation *not* recognised by the Commission to ensure that these are satisfactory.	No exceptions noted.
3	There is a regular – at least annual – assessment of whether third countries or international organisations to which personal data are transferred are still recognised by the Commission.	Asked Management whether personal data are transferred to recognised third countries/international organisations. Inspected documentation that the processor regularly – at least annually – ensures that a third country or international organisation to which personal data are transferred is still recognised by the Commission.	No exceptions noted.
4	There is a regular – at least annual – assessment of 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.	Asked Management whether personal data are transferred to third countries/international organisations that are *not* recognised. Inspected documentation that the processor regularly – at least annually– assesses whether the appropriate safeguards etc. from third countries or international organisations that are *not* recognised and to which personal	No exceptions noted.

Control objective:

Procedures and controls have been established 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.	Assembles control activity	Control tests performed by PwC	Result of PwC's test
		data are transferred are still sufficient, can be enforced and are effective.	
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.	Inspected documentation that 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.	No exceptions noted.