



Visma e-conomic A/S

Independent auditor's ISAE 3000 type 2 assurance report on information security and measures pursuant to the data processing agreement with customers using e-conomic throughout the period from 1 January 2025 to 31 December 2025

Table of contents

- 1. Independent auditor’s report 1
- 2. Management assertion4
- 3. Description of processing.....6
- 4. Visma e-conomic’s control objectives, controls, test and results 14

1. Independent auditor's report

To: Visma e-conomic A/S and Visma e-conomic A/S' customers

Scope

We have been engaged to provide assurance about Visma e-conomic A/S' (hereinafter "e-conomic") description in section 3 of the described services in accordance with the data processing agreements with customers throughout the period from 1 January 2025 to 31 December 2025 (hereinafter "the description"), and about the design, implementation and operation of controls related to the control objectives stated in the description.

e-conomic uses the following sub-processors: Google Cloud Platform, Microsoft Azure, Twilio, Actito SA, 84codes AB, Orca security Ltd., Mailjet SAS, KMD A/S, Cloudflare Inc, Visma Software International AS, Visma Solutions OY, MySupply ApS and Visma Dataløn A/S. e-conomic's system description does not include control objectives and associated controls at the sub-service organisations. This report is prepared using the carve-out method, and our testing does not include controls that are carried out by the sub-processors.

Some of the control objectives described in e-conomic's description of its system can only be achieved if the complementary controls at the user organisations are suitably designed and operating effectively together with the controls at e-conomic. The opinion does not include the suitability of the design and operating effectiveness of these complementary controls.

e-conomic's responsibilities

e-conomic is responsible for preparing the description and the accompanying statement in section 2, including the completeness, accuracy and method of presentation of the description and the 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.

Auditor's independence and quality control

We have complied with the requirements for independence in the IESBA's Code of Ethics for Professional Accountants, which is based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional conduct.

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

Auditor's responsibilities

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

We conducted our engagement in accordance with International Standard on Assurance Engagements 3000, "Assurance Engagements Other than Audits or Reviews of Historical Financial Information", and additional requirements under Danish audit regulation to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are appropriately designed and operating effectively.

An assurance engagement to report on the description, design and implementation of controls at a data processor involves performing procedures to obtain evidence about the disclosures in e-conomic's de-

description of its services, and the design, implementation and operation of controls. The procedures selected depend on the auditor's judgement, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the design and operating effectiveness of controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved.

An assurance engagement of this type also includes evaluating the overall presentation of the description, the appropriateness of the objectives stated therein, and the appropriateness of the criteria specified by the data processor and described in section 2.

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

Limitations of controls at e-conomic

e-conomic's description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of control that the individual data controllers may consider important in their particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect personal data breaches. Furthermore, the projection of any evaluation of the controls to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Opinion

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

- (a) The description fairly presents the services provided as designed and implemented throughout the period from 1 January 2025 to 31 December 2025;
- (b) The controls related to the control objectives stated in the description were suitably designed and implemented throughout the period from 1 January 2025 to 31 December 2025.
- (c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period from 1 January 2025 to 31 December 2025.

Description of tests of controls

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

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 e-economic's application (e-economic) who have a sufficient understanding to consider it along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the EU Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "the Regulation") have been complied with.

Copenhagen, 4 February 2026

Deloitte

Statsautoriseret Revisionspartnerselskab

CVR No. 33 96 35 56

Thomas Kühn

Partner, State-Authorised Public Accountant

2. Management assertion

The accompanying description has been prepared for e-economic customers who have used the services described in this report, and who have a sufficient understanding to consider the description along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the Regulation have been complied with.

e-economic uses the following sub-processor: Google Cloud Platform, Microsoft Azure, Twilio, Actito SA, 84codes AB, Orca security Ltd., Mailjet SAS, Cloudflare Inc, KMD A/S, Visma Software International AS, Visma Solutions OY, MySupply ApS and Visma Dataløn A/S.. e-economic's system description does not include control objectives and associated controls at the sub-service organisations. This report is prepared using the carve-out method, and our testing does not include controls that are carried out by the sub-processors.

Some of the control objectives described in e-economic's description of its system can only be achieved if the complementary controls at the user organisations are suitably designed and operating effectively together with the controls at e-economic. The opinion does not include the suitability of the design and operating effectiveness of these complementary controls.

e-economic confirms that:

- a) The accompanying description in section 3 fairly presents e-economic, which has processed personal data for data controllers covered by the General Data Protection Regulation throughout the period from 1 January 2025 to 31 December 2025. The criteria used in making this statement were that the accompanying description:
 - (i) Presents how the services delivered were designed and implemented, including:
 - The types of services provided, including the type of personal data processed;
 - The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete and restrict processing of personal data;
 - The procedures used to ensure that data processing has taken place in accordance with contract, instructions or agreement with the data controller;
 - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality;
 - The procedures which, on termination of data processing, ensure that, according to the data controller's choice, all personal data can be deleted or returned, unless retention of such personal data is required by law or regulation;
 - The procedures which, in the event of a personal data breach, support the data controller in reporting to the supervisory authority and notifying the data subjects of the breach;
 - The procedures which ensure appropriate technical and organisational security measures for the processing of personal data, taking into account the risks involved in processing, in particular, by accidental or illegal destruction, loss, alteration, unauthorised disclosure or access to personal data transmitted, stored or otherwise processed;
 - Controls which we, referring to the system, assumed would be designed and implemented by the data controller and which, if necessary, to achieve the control objectives set forth in the description, are identified in the description;
 - Other aspects of our control environment, risk assessment process, information system (including related business processes) and communication, control activities, and monitoring controls that are relevant to the processing of personal data.
 - (ii) Contains relevant information about changes in the data processor's services in the processing of personal data made throughout the period from 1 January 2025 to 31 December 2025.

- (iii) Does not omit or distort information relevant to the scope of e-conomic described for the processing of personal data, taking into consideration that the description was prepared to meet the general needs of a wide range of data controllers and therefore cannot include any aspect of the system that the individual data controller might consider important according to their particular circumstances.
- b) The controls associated with the control objectives listed in the accompanying description were appropriately designed and implemented throughout the period from 1 January 2025 to 31 December 2025. 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.
 - (iii) The controls were consistently applied as designed and that manual controls were performed by persons with appropriate competence and skills throughout the period from 1 January 2025 to 31 December 2025.
- c) Appropriate technical and organisational measures have been established and maintained to comply with agreements with the data controllers, good data processing practices and relevant data processing requirements under the General Data Protection Regulation.

Copenhagen, 4 February 2026

Visma e-conomic A/S

Karina Wellendorph
Managing Director

3. Description of processing

3.1 About e-economic and the Visma Group

e-economic, a software company specialising in cloud-based solutions for ERP, electronic invoicing and accounting helps over 260,000 businesses in the Danish market streamline their operations. With over two decades of experience, e-economic has been a driving force in the digitalisation of accounting and finance, offering key features such as digital document handling, invoicing and automatic bank transaction reconciliation.

e-economic is a subsidiary of Visma, a Norwegian-headquartered provider of essential business software dedicated to supporting a more efficient and resilient society. Visma empowers companies and organisations of all sizes to simplify their work, enabling growth and prosperity. With over 16,000 employees, Visma supports 2.1 million customers across the Nordics, Benelux, Central and Eastern Europe and Latin America, all united by a shared commitment to **make progress happen**.

Recognising its role as a provider of mission-critical systems, Visma places great importance on information security and the protection of customer and employee privacy. Consequently, Visma is continuously enhancing its security and data protection procedures and practices throughout the entire organisation.

3.2 Organisation of Data Protection

3.2.1 Data protection in e-economic

e-economic maintains a dedicated GRC (Governance, Risk and Compliance) that ensures adherence to all relevant data protection laws and regulations, including the General Data Protection Regulation (GDPR). This team is responsible for overseeing policies and procedures related to data protection, security and GDPR compliance, in addition to managing other legal aspects that support both customers and employees.

3.2.2 Data Protection Organisation

Visma, as the parent company of e-economic, implements a comprehensive data protection program. Data Protection Managers (DPMs) are assigned within each Visma company, including e-economic, to oversee local data protection efforts. All Data Protection Managers are trained individually and through specific workshops. These DPMs receive support and guidance from the Visma Group Legal & Compliance Team, which also provides regular reports to the Board of Directors via the Risk Audit Committee. This structure ensures that data protection is managed at both the company and group levels, supported by clear policies, mandatory annual assessments of products and services, and continuous monitoring through a security and compliance regime.

In e-economic, the appointed DPM is a member of the GRC team.

3.2.3 Each employee

Every Visma employee is integral to upholding the Visma Data Protection Framework in their daily tasks, recognising that individual contributions are essential for ensuring data protection and privacy.

Employees at e-economic are educated on these responsibilities during onboarding and are continually reinforced through ongoing internal GDPR awareness campaigns and training. All employees receive annual data protection awareness training, with specialised training provided for specific roles. Furthermore, confidentiality clauses are included in all employee contracts, remaining in effect even after their employment concludes.

3.3 Scope of audit

This audit focuses on e-economic's role as a data processor for the accounting software it develops and sells in Denmark.

3.3.1 Description of processing

e-economic responsibly processes personal data on behalf of its customers, who, in turn, act as the data controllers for the data they process within the e-economic application.

This processing is formally established and governed by a comprehensive data processing agreement between e-economic and each customer. The primary purpose of this processing is to ensure that customers can effectively use the e-economic application, and that the terms of the data processing agreement are fully met. This agreement, which outlines the specifics of data processing, is readily accessible on e-economic's website and directly within each customer's e-economic application.

3.3.2 e-economic application description

e-economic is a cloud-based accounting application, developed and offered by e-economic, and designed to empower small and medium-sized businesses in Denmark to manage their accounting and bookkeeping practices in full compliance with Danish law. Via integrations to third-party applications such as time management tools, booking systems and inventory management software, it is possible to achieve an all-around administration solution for a business. For growing companies, the system also offers the flexibility to scale up and incorporate ERP functionalities.

Within the e-economic application, customers can seamlessly handle essential tasks including invoicing, sales management, finance operations, bookkeeping, VAT accounts, financial statements and detailed reporting. In facilitating these services, personal information can be added within the e-economic application, which e-economic then processes on behalf of the customer in its capacity as a data processor.

3.3.3 Data sub-processors

In order to provide the e-economic application to customers, e-economic engages various sub-processors, including third parties and other companies within the Visma group. Customers provide their prior general written approval for the use of these sub-processors when signing the Data Processing Agreement (DPA). e-economic ensures that all engaged sub-processors adhere to data protection obligations equivalent to those stipulated in the DPA. In the cases where e-economic introduces a new sub-processor, customers are notified 30 days in advance, providing the customer with the right to object if the new sub-processor is deemed not to process data in accordance with applicable data protection legislation. Any transfer of personal data to third countries is secured via valid mechanisms.

Details regarding the sub-processors that e-economic engages with are provided within the data processing agreement established with customers. This agreement clearly states that customers have granted their general consent for e-economic to either change existing sub-processors or engage new ones. Importantly, e-economic commits to informing its customers in advance before integrating any new sub-processors, maintaining transparency and trust throughout the processing chain.

e-economic engages with the following sub-processors for the purposes described below:

Sub-processor	Purpose
84codes AB	When customers send emails or invoices through our application, CloudAMQP functions as the underlying queuing system.
Actito SA	MessageCloud by SmartFocus supports the sending of emails generated through the e-economic application.
Google Ireland Limited	The Google Cloud Platform hosts the e-economic application and database servers.
Microsoft Ireland Operations Limited	Microsoft Azure hosts e-economic's database backup.
Twilio	SendGrid supports sending emails and invoices generated through the e-economic application.
Orca security Ltd.	The Orca Cloud Security Platform is used for infrastructure security by monitoring configurations and data.
Mailjet SAS	Mailgun supports the receiving of emails and invoices sent to e-economic.
Cloudflare, Inc.	Cloud Security Posture Management supports security management in the cloud.

The following sub-processors are engaged only for customers who choose to use the specific services.

Sub-processor	Purpose
KMD A/S	KMD receives and forwards VANS EDI messages to and from e-economic.
Visma Software International AS	Visma Software International supports the AutoSuggest functionality for bank reconciliation, Smartscan for the automatic scanning of documents, and Visma Document Storage for document retention.
Visma Solutions OY	AutoInvoice is used when customers send e-invoices and documents through the Peppol network.
MySupply ApS	VAX360 is used when customers send e-invoices and documents to recipients in Finland.
Visma Dataløn A/S	Dataløn supports payroll administration.

3.3.4 The nature of processing

In general, e-economic processes ordinary personal data, which may include name, job title, email address and phone number. However, e-economic does not control the specific categories of personal data customers added to the application. Therefore, the types of data processed vary by customer agreement. It is possible that customers may process sensitive personal data within e-economic, including information related to health, sexual orientation or trade union membership.

Additionally, depending on how our customers use e-conomic, e-conomic may process several categories of data subjects, such as:

- Data controller's end-users
- Data controller's employees
- Data controller's contact person
- Data controller's customers
- Data controller's suppliers.

It is important to note that other categories of data subjects may also be processed, depending on the specific use of e-conomic by each customer.

3.3.5 Risk assessment

e-conomic believes that effective risk management integrated with all organisational processes contributes to the achievement of objectives and improved performance in the working environment, security, legal and regulatory compliance, product quality, project management, operational effectiveness, governance and corporate reputation. To determine risk, e-conomic uses the risk = impact x likelihood methodology, with risk, impact and likelihood levels appropriate to e-conomic and its customers. Risk levels take into account information about the asset and/or data being protected, its value, vulnerabilities and threats against it.

By identifying all relevant risks that threaten the security and privacy of information, e-conomic is able to maintain an acceptable level of risk through the implementation of technical and organisational controls. Risk management at e-conomic is implemented on multiple levels.

3.3.6 3.5.1 Security Forum

Risk management at e-conomic is implemented on multiple levels. On a high level, the Security Forum in e-conomic evaluates risks within the scope of privacy and security and documents them in a risk register. All members of the forum add to the risk register on a continuous basis, and based on impact and likelihood, the risks are treated accordingly.

3.3.7 Visma Risk Score

Additionally, Visma utilises a comprehensive Risk Score to provide a consolidated and continuous overview of a company's performance against Visma's requirements across critical areas such as legal compliance (including vendor management), security, sustainability and training & awareness. This framework centralises insights into a company's risk profile, helping to ensure focused attention on relevant risk areas based on data and clear visualisation.

The Security Score specifically provides e-conomic with a clear overview of the security status for the e-conomic application and infrastructure. Its purpose is to assist e-conomic in prioritising security efforts. This score is calculated based on data from the Visma Security Program, taking into account all security services implemented and the security issues that remain unresolved. Actions to be taken are generated as tickets, which are prioritised based on risk to customers and e-conomic.

The Legal Score supports e-conomic in identifying potential risks related to compliance for various legislation, including data protection. A key tool in evaluating the Legal Risk Score is the Compliance Self-Assessment (CSA). This assessment comes in two parts: one for the e-conomic Legal Unit, which evaluates broader compliance topics such as data protection, cookies, vendor management and AI; and another for the Product, focusing on data protection controls within the e-conomic application related to areas such as access to data, APIs, log data, data deletion, data restore, anonymisation, privacy breaches, data subject rights and privacy by design and default. The results of the CSA directly contribute to the Legal Score for e-conomic, with the score being regularly followed up by management and the board.

3.3.8 Risk Management of third-party vendors

This comprehensive approach to risk management extends to third-party providers through Visma's Vendor Management Framework. This framework is mandatory for critical and strategic vendors, particularly those handling sensitive personal data or essential operations. It involves annual or regular risk assessments using audit templates and questionnaires, supported by contractual safeguards, due diligence and continuous monitoring. Notably, vendor management is always required for vendors processing personal data, regardless of their critical designation. e-conomic strictly avoids engaging vendors with unacceptable risks, and all international data transfers are secured via valid mechanisms. Based on these assessments, risks are identified and assessed by e-conomic.

3.3.9 Control measures

e-conomic has implemented controls regarding the processing of personal data in the following areas:

- Data processing agreements and instructions (control objective A)
- Technical security measures (control objective B)
- Organisational measures (control objective C)
- Erasure and return of personal data (control objective D)
- Retention of personal data (control objective E)
- Use of sub-processors (control objective F)
- Transfer to third countries (control objective G)
- Assistance to the data controller (control objective H)
- Security breach management (control objective I).

The control measures that e-conomic deems relevant to the processing of personal data are presented in section 5. A detailed description of relevant control measures is available below.

3.3.10 Data processing agreements and instructions (control objective A)

Procedures and controls are complied with to ensure that instructions for the processing of personal data are applied consistently and in line with the data processing agreement entered into.

e-conomic has prepared several procedures describing how personal data are to be processed to ensure secure processing in relation to confidentiality, integrity and availability. Furthermore, these procedures emphasise the importance of personal data only being processed based on instruction from the data controller. Employees are informed about this on an ongoing basis through various internal GDPR awareness campaigns, including an annual e-learning course. New employees are also obligated to participate in a mandatory GDPR session where they are informed about how to process personal data in accordance with general data protection laws as well as the data processing agreement that e-conomic enters into with its customers.

3.3.11 Technical security measures (control objective B)

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

By identifying all relevant risks that threaten the security and privacy of information, e-conomic is able to maintain an acceptable level of risk through the implementation of technical controls in accordance with the data processing agreements in place. These security measures are implemented throughout e-conomic's supply chain, and sub-processors are audited to ensure compliance with these controls annually.

To ensure a continuous evaluation on the level of the technical security measures in place, e-conomic undergoes an annual assessment covering the implemented security measures. These measures include having procedures for access control, enforcing password policies, encrypting data, detecting and responding to software vulnerabilities, having procedures for testing and quality assurance procedures, monitoring logs and updating software as needed.

3.3.12 Organisational measures (control objective C)

Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.

Based on the risk assessments mentioned above, e-economic has implemented several organisational measures. In order to maintain information security at all levels in the organisation, from support cases and data in the cloud to the confidentiality of business relations, e-economic maintains a common Group-wide Information Security Policy. This Information Security Policy is updated annually and is available to all employees on e-economic's intranet.

Prior to employment, e-economic ensures that employees understand their responsibilities, and that they are suitable for the roles for which they are considered. Screening is carried out by the hiring manager in collaboration with HR. Upon being hired, employees must sign a confidentiality agreement within their employment contract and are required to read the Employee Handbook and Information Security Policy before their first day.

All new employees participate in an onboarding session where the Information Security Policy along with data protection policies are presented. Throughout the employment, awareness training is carried out on an ongoing basis in order to ensure that employees continue to process personal data in accordance with the data processing agreement e-economic enters into with customers. e-economic has a dedicated GRC team that supports the rest of the organisation with questions related to GDPR.

Upon termination of employment at e-economic, employees are issued a written reminder of their continuing duty of confidentiality, which they are required to sign.

3.3.13 Erasure and return of personal data (control objective D)

Procedures and controls are complied with to ensure that personal data can be deleted or returned if arrangements are made with the data controller to this effect.

e-economic has established procedures for the deletion of personal data. Upon the termination of a customer's agreement, including those terminated due to non-payment, all customer-owned data in the production database are scheduled for deletion after a retention period of five years plus the remaining portion of the financial year for any given transaction, in accordance with Section 15 of the Danish Bookkeeping Act. This deletion policy also applies to trial agreements.

While an e-economic agreement is active, customers have the option to delete and anonymise their own personal data directly within the application. For personal data pertaining to their customers, anonymisation is permitted; however, direct deletion of these data are restricted to prevent miscalculations of account balances within the e-economic application. If any personal data are subject to the documentation requirements of Section 15 of the Danish Bookkeeping Act, customers can only delete or anonymise these specific data after a retention period of five years plus the remainder of the financial year in which the request for deletion is made. Regardless of these data retention policies, customers always retain the ability to delete other users from their agreement who no longer require access to the accounting data or lack a legitimate purpose for such access.

3.3.14 Storage of personal data (control objective E)

Procedures and controls are complied with to ensure that the data processor will only store personal data in accordance with the agreement with the data controller.

Personal data are retained by e-economic for the duration of the customer relationship and for an additional five years plus the remaining financial year for any given transaction, as required by Section 15 of the Danish Bookkeeping Act.

3.3.15 Use of sub-processors (control objective F)

Procedures and controls are complied with to ensure that only approved sub-processors are used and that, when following up on such sub-processor's technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processors ensure adequate security of processing.

Customers provide e-conomic with general consent to change or engage sub-processors. e-conomic maintains a comprehensive and updated overview of all sub-processors, accessible within its standard data processing agreement. e-conomic ensures that all sub-processors are bound by data processing agreements imposing conditions and requirements equivalent to those in e-conomic's agreements with its customers. To ensure ongoing compliance, e-conomic regularly monitors, reviews and audits all sub-processors through questionnaires and/or by reviewing auditor's reports.

3.3.16 Transfer to third countries (control objective G)

Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.

e-conomic has procedures in place to ensure that the transfer of personal data to third countries takes place in accordance with the data processing agreement entered into with its customers.

When transferring personal data to a third country, e-conomic makes sure to implement an appropriate legal transfer mechanism on the basis of e.g. an adequacy decision, for instance with the EU-US Data Privacy Framework, or EU Standard Contractual Clauses (SCC) with appropriate safeguards and performing a Transfer Impact Assessment (TIA).

3.3.17 Assistance to data controller (control objective H)

Procedures and controls are complied with to ensure that the data processor can assist the data controller in handing out, correcting, deleting or restricting information on the processing of personal data to the data subject.

e-conomic has prepared procedures for assisting the data controller with the delivery, correction and deletion of personal data. The purpose of these procedures is to ensure that data controllers can fulfil their duties towards data subjects.

3.3.18 Security breach management (control objective I)

Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into.

e-conomic has established comprehensive procedures for handling both potential and actual security breaches. All employees are fully aware of these procedures, understanding their critical role in reporting security incidents. All incidents are logged in an incident register. Furthermore, the GRC team is actively involved in managing all incidents that concern personal data.

A dedicated Crisis Communication team ensures that communication to customers regarding incidents is managed effectively and in full accordance with the data processing agreement. Upon request, e-conomic will assist its customers by providing all relevant information deemed necessary for notifying the Data Protection Authorities.

3.3.19 Complementary data controller controls

e-conomic is designed on the assumption that certain controls should be implemented and operated effectively by the customer to achieve certain control objectives in this audit.

Customers of e-economic should consider whether the following complementary controls have been implemented and operated effectively within their own organisations:

- Controls to ensure that physical access to the customer's premises is restricted to authorised individuals
- Controls to ensure that the customer organisation has proper control over the use of IDs and passwords that are used for accessing information in e-economic
- Controls to ensure that the access right assignments for e-economic are provided adequately and in compliance with the user's work-related needs.

Furthermore, it is the customer's responsibility to ensure that their processing of personal data happens in accordance with the GDPR. While e-economic has features in place designed to assist its customers in their compliance with the GDPR, it is ultimately the responsibility of Visma e-economic customers to:

- Ensure that there is a legal basis for processing personal data within e-economic
- Delete or anonymise personal data when required to do so by the GDPR
- Ensure that the personal data processed in e-economic is correct and up to date
- Respond to requests coming from the data subject
- Ensure that the data subjects are informed about the processing of personal data
- Restrict access to personal data
- Minimise the amount of personal data processed to necessary data only.

For the avoidance of doubt, this means that it is the customer's own responsibility to change and/or anonymise data within the e-economic application.

4 Visma e-conomic's control objectives, controls, test and results

Introduction

This report is intended to provide the data controllers with information about the controls at e-conomic that may affect the processing of personal data, and to provide the data controllers with information about the design, implementation, and operation of the controls that were tested.

This report, when combined with an understanding and assessment of the controls at the data controllers, is intended to assist the data controllers in assessing the risks related to the processing of personal data that may be affected by the controls at e-conomic.

e-conomic uses the following sub-processors: Google Cloud Platform, Microsoft Azure, Twilio, Actito SA, 84codes AB, Orca security Ltd., and Mailjet SAS, Cloudflare Inc, KMD A/S, Visma Software International AS, Visma Solutions OY, MySupply ApS and Visma Dataløn A/S. e-conomic's system description does not include control objectives and associated controls at the sub-service organisations. This report is prepared using the carve-out method, and our testing does not include controls that are carried out by the sub-processors.

Our testing of e-conomic's controls was limited to the control objectives and related controls listed in the matrices in this section of the report and did not include all controls described in the system description, nor controls that may be in place at the data controllers. It is the responsibility of the data controllers to evaluate this information in relation to the controls in place at each data controller. If certain complementary controls are not in place at the data controller, e-conomic's controls may not compensate for such weaknesses.

Test of controls

The test of controls performed involves one or more of the following methods:

Method	Description
Interview	Interviews with selected personnel at e-conomic.
Observation	Observation of the execution of controls.
Inspection	Review and evaluation of policies, procedures and documentation of the performance of the control. This includes reading and evaluating reports and other documentation to assess whether specific controls are designed and implemented. Furthermore, it is assessed whether controls are monitored and supervised adequately and at appropriate intervals.
Re-performance	Repetition of the relevant control to verify that the control functions as intended.

Control objectives, controls, and test results

The following matrices state the control objectives and controls tested and present the audit procedures performed and the results thereof. If we identified material control weaknesses, we have described them as well.

Control objective A

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

No.	e-economic's control activity	Test performed by Deloitte	Results of Deloitte's test
A.1	<p>Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Deloitte has checked by way of inspection that formalised procedures exist to ensure that personal data are only processed according to instructions.</p> <p>Deloitte has checked by way of inspection that the procedures include a requirement to assess, at least once a year, the need for updates, including in case of changes in the data controller's instructions or changes in the data processing.</p> <p>Deloitte has checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
A.2	<p>The data processor only processes personal data stated in the instructions from the data controller.</p> <p>Data controllers who use the e-economic application enter into an agreement regarding instructions as part of Standard DPA.</p> <p>Data controllers who enter into separate or specific DPAs also follow the overall instructions entered into.</p>	<p>Deloitte has checked by way of inspection that Management ensures that personal data are only processed according to instructions.</p> <p>Deloitte has inspected a sample of data processing agreements and checked that processes of personal data take place in accordance with instructions.</p>	No exceptions noted.
A.3	The data processor immediately informs the data controller if an instruction, in the data processor's opinion, infringes the Regulation or other European Union or member state data protection provisions.	Deloitte has checked by way of inspection that formalised procedures exist ensuring verification that personal data are not processed against the Regulation or other legislation.	<p>We have been informed that there have not been any instructions during the period that the data processor has deemed unlawful.</p> <p>No exceptions noted.</p>

Control objective A**Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with in accordance with the data processing agreement entered into.**

No.	e-economic's control activity	Test performed by Deloitte	Results of Deloitte's test
A.3		<p>Deloitte has checked by way of inspection that procedures are in place for informing the data controller of cases where the processing of personal data is evaluated to be against legislation.</p> <p>Deloitte has checked by way of inspection that the data controller was informed in cases where the processing of personal data was evaluated to be against legislation.</p>	

Control objective B**Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant security of processing.**

No.	e-conomic's control activity	Test performed by Deloitte	Results of Deloitte's test
B.1	<p>Written procedures exist which include a requirement that safeguards agreed are established for the processing of personal data in accordance with the agreement with the data controller.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Deloitte has checked by way of inspection that formalised procedures exist to ensure establishment of the safeguards agreed.</p> <p>Deloitte has checked by way of inspection that procedures are up to date.</p> <p>Deloitte has checked by way of inspection that the agreed safeguards have been established for a sample of data processing agreements.</p>	No exceptions noted.
B.2	<p>The data processor has performed a risk assessment and, based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of the safeguards agreed with the data controller.</p> <p>Risk assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Deloitte has checked by way of inspection that formalised procedures are in place to ensure that the data processor performs a risk assessment to achieve an appropriate level of security.</p> <p>Deloitte has checked by way of inspection that the risk assessment performed is up to date and comprises the current processing of personal data.</p> <p>Deloitte has checked by way of inspection that the data processor has implemented technical measures ensuring an appropriate level of security consistent with the risk assessment.</p> <p>Deloitte has checked by way of inspection that the data processor has implemented the safeguards agreed with the data controller.</p>	No exceptions noted.

Control objective B**Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant security of processing.**

No.	e-conomic's control activity	Test performed by Deloitte	Results of Deloitte's test
B.3	For the systems used in the processing of personal data, antivirus software has been installed and is updated on a regular basis.	<p>Deloitte has checked by way of inspection that, for the systems used in the processing of personal data, antivirus software has been installed.</p> <p>Deloitte has checked by way of inspection that antivirus software is up to date.</p>	No exceptions noted.
B.4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	<p>Deloitte has checked by way of inspection that external access to systems and databases used in the processing of personal data takes place only through a secured firewall.</p> <p>Deloitte has checked by way of inspection that the firewall has been configured in accordance with the relevant internal policy.</p>	No exceptions noted.
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	<p>Deloitte has checked by way of inspection that internal networks are segmented to ensure limited access to systems and databases used in the processing of personal data.</p> <p>Deloitte has checked by way of inspection documentation to ensure appropriate network segmentation.</p>	No exceptions noted.
B.6	Access to personal data is isolated to users with a work-related need for such access.	<p>Deloitte has checked by way of inspection that formalised procedures are in place for restricting user access to personal data.</p> <p>Deloitte has checked by way of inspection that formalised procedures are in place for following up on users' accesses to personal data being consistent with their work-related need.</p>	No exceptions noted.

Control objective B**Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant security of processing.**

No.	e-conomic's control activity	Test performed by Deloitte	Results of Deloitte's test
		<p>Deloitte has checked by way of inspection that the technical measures agreed support retaining the restriction in users' work-related access to personal data.</p> <p>Deloitte has checked by way of inspection of a sample of user's access to systems and databases that such access is restricted to the employee's work-related need.</p>	
B.7	For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature.	<p>Deloitte has checked by way of inspection that, for systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature.</p> <p>Deloitte has checked by way of inspection that, in a sample of alarms, these were followed up on and that the data controllers were informed thereof as appropriate.</p>	No exceptions noted.
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	<p>Deloitte has checked by way of inspection that formalised procedures are in place to ensure that transmissions of sensitive and confidential data through the internet are protected by powerful encryption based on a recognised algorithm.</p> <p>Deloitte has checked by way of inspection that technological encryption solutions have been available and active throughout the assurance period.</p>	No exceptions noted.

Control objective B**Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant security of processing.**

No.	e-conomic's control activity	Test performed by Deloitte	Results of Deloitte's test
		<p>Deloitte has checked by way of inspection that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.</p> <p>Deloitte has inquired whether any unencrypted transmission of sensitive and confidential personal data has taken place during the assurance period and whether the data controllers have been appropriately informed thereof.</p>	
B.9	<p>Logging of the following matters has been established in systems, databases and networks:</p> <ul style="list-style-type: none">• Activities performed by system administrators and others holding special rights;• Security incidents comprising:<ul style="list-style-type: none">○ Changes in log set-ups, including disabling of logging;○ Changes in users' system rights;○ Failed attempts to log on to systems, databases or networks. <p>Logon data are protected against manipulation and technical errors and are reviewed regularly.</p>	<p>Deloitte has checked by way of inspection that formalised procedures exist for setting up logging of user activities in systems, databases or networks that are used to process and transmit personal data, including review of and follow-up on logs.</p> <p>Deloitte has checked by way of inspection that logging of user activities in systems, databases or networks that are used to process or transmit personal data has been configured and activated.</p> <p>Deloitte has checked by way of inspection that user activity data collected in logs is protected against manipulation or deletion.</p> <p>Deloitte has checked by way of inspection of a sample of days of logging that the content of log files is as expected compared to the set-up and that documentation exists regarding the follow-up performed and the response to any security incidents.</p>	No exceptions noted.

Control objective B**Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant security of processing.**

No.	e-conomic's control activity	Test performed by Deloitte	Results of Deloitte's test
B.10	Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form. Such use only takes place to accomplish the data controller's purpose according to agreement and on the data controller's behalf.	<p>Deloitte has checked by way of inspection that formalised procedures exist for using personal data for development, testing or similar activity to ensure that such use only takes place in pseudonymised or anonymised forms.</p> <p>Deloitte has checked by way of inspection of a sample of development or test databases that personal data included therein is pseudonymised or anonymised.</p> <p>Deloitte has checked by way of inspection of a sample of development or test databases in which personal data are not pseudonymised or anonymised that this has taken place according to agreement with, and on behalf of, the data controller.</p>	No exceptions noted.
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	<p>Deloitte has checked by way of inspection that formalised procedures exist for regularly testing technical measures, including for performing vulnerability scans and penetration tests.</p> <p>Deloitte has checked by way of inspection of samples that documentation exists regarding regular testing of the technical measures established.</p> <p>Deloitte has checked by way of inspection that any deviations or weaknesses in the technical measures have been responded to in a timely and satisfactory manner and communicated to the data controllers as appropriate.</p>	No exceptions noted.

Control objective B**Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant security of processing.**

No.	e-conomic's control activity	Test performed by Deloitte	Results of Deloitte's test
B.12	Changes to systems, databases or networks are made consistently with procedures established that ensure maintenance using relevant updates and patches, including security patches.	<p>Deloitte has checked by way of inspection that formalised procedures exist for handling changes to systems, databases or networks, including handling of relevant updates, patches and security patches.</p> <p>Deloitte has checked by way of inspection of extracts from technical security parameters and set-ups that systems, databases, or networks have been updated using agreed changes and relevant updates, patches and security patches.</p>	No exceptions noted.
B.13	A formalised procedure is in place for granting and removing user access to personal data. User access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.	<p>Deloitte has checked by way of inspection that formalised procedures exist for granting and removing user access to systems and databases used to process personal data.</p> <p>Deloitte has checked by way of inspection of a sample of employee's access to systems and databases that the user's access granted has been authorised and that a work-related need exists.</p> <p>Deloitte has checked by way of inspection of a sample of resigned or dismissed employees that their access to systems and databases was deactivated or removed in a timely manner.</p> <p>Deloitte has checked by way of inspection that documentation exists that user access granted is evaluated and authorised on a regular basis – and at least once a year.</p>	No exceptions noted.

Control objective B**Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant security of processing.**

No.	e-conomic's control activity	Test performed by Deloitte	Results of Deloitte's test
B.14	Systems and databases processing personal data that involve a high risk for the data subjects are accessed as a minimum by using two-factor authentication.	<p>Deloitte has checked by way of inspection that formalised procedures exist to ensure that two-factor authentication is applied in the processing of personal data that involves a high risk for the data subjects.</p> <p>Deloitte has checked by way of inspection that user access to processing personal data that involve a high risk for the data subjects can only take place by using two-factor authentication.</p>	No exceptions noted.
B.15	Physical access safeguards have been established so as to only permit physical access by authorised persons to premises and data centres at which personal data are stored and processed.	<p>Deloitte has checked by way of inspection that formalised procedures exist to ensure that only authorised persons can gain physical access to premises and data centres at which personal data are stored and processed.</p> <p>Deloitte has checked by way of inspection of documentation that, throughout the assurance period, only authorised persons have had physical access to premises and data centres at which personal data are stored and processed.</p>	No exceptions noted.

Control objective C**Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to ensure relevant security of processing.**

No.	e-conomic's control activity	Test performed by Deloitte	Results of Deloitte's test
C.1	<p>Management of the data processor has approved a written information security policy that has been communicated to all relevant stakeholders, including the data processor's employees. The IT security policy is based on the risk assessment performed.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.</p>	<p>Deloitte has checked by way of inspection that an information security policy exists which management has considered and approved within the assurance period.</p> <p>Deloitte inspected documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.</p>	No exceptions noted.
C.2	Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.	<p>Deloitte inspected documentation showing management's assessment of the information security policy, and that the policy generally meets the requirements for safeguarding data in relation to the data processing agreements entered into.</p> <p>Deloitte has checked by way of inspection of a sample of data processing agreements that the requirements in the agreements are covered by the requirements of the information security policy for safeguards and security of processing.</p>	No exceptions noted.
C.3	<p>The employees of the data processor are screened as part of the employment process. Such screening comprises, as relevant:</p> <ul style="list-style-type: none">• Assessment of CV.	<p>Deloitte has checked by way of inspection that formalised procedures are in place to ensure screening of the data processor's employees as part of the employment process.</p> <p>Deloitte has checked by way of inspection of a sample of new employees during the assurance period that documentation exists of the screening having comprised:</p> <ul style="list-style-type: none">• Assessment of CV.	No exceptions noted.

Control objective C Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to ensure relevant security of processing.			
No.	e-economic's control activity	Test performed by Deloitte	Results of Deloitte's test
C.4	Upon appointment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data.	<p>Deloitte has checked by way of inspection of a sample of new employees during the assurance period that the relevant employees have signed a confidentiality agreement.</p> <p>Deloitte has checked by way of inspection of a sample of new employees during the assurance period that the relevant employees have been introduced to:</p> <ul style="list-style-type: none"> • Information security policy; • Procedures for processing data and other relevant information. 	No exceptions noted.
C.5	For resignations or dismissals, the data processor has implemented a process to ensure that users' rights are deactivated or terminated, and that assets are returned.	<p>Deloitte has inspected procedures ensuring that resigned or dismissed employees' rights are deactivated or terminated upon resignation or dismissal and that assets such as access cards, computers, mobile phones, etc. are returned.</p> <p>Deloitte has checked by way of inspection of a sample of employees resigned or dismissed during the assurance period that rights have been deactivated or terminated and that assets have been returned.</p>	No exceptions noted.
C.6	Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers.	<p>Deloitte has checked by way of inspection that formalised procedures exist to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality.</p> <p>Deloitte has checked by way of inspection of a sample of employees resigned or dismissed</p>	No exceptions noted.

Control objective C**Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to ensure relevant security of processing.**

No.	e-conomic's control activity	Test performed by Deloitte	Results of Deloitte's test
		during the assurance period that documentation exists of the continued validity of the confidentiality agreement and the general duty of confidentiality.	
C.7	Awareness training is provided to the data processor's employees on a regular basis with respect to general IT security and security of processing related to personal data.	Deloitte has checked by way of inspection that the data processor provides awareness training to the employees covering general IT security and security of processing related to personal data. Deloitte inspected documentation that employees who have either access to or process personal data have completed the awareness training provided.	No exceptions noted.

Control objective D			
Procedures and controls are complied with to ensure that personal data can be deleted or returned if arrangements are made with the data controller to this effect.			
No.	e-economic's control activity	Test performed by Deloitte	Results of Deloitte's test
D.1	<p>Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Deloitte has checked by way of inspection that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller.</p> <p>Deloitte has checked by way of inspection that the procedures are up to date.</p>	No exceptions noted.
D.2	<p>The following specific requirements have been agreed with respect to the data processor's storage periods and deletion routines:</p> <ul style="list-style-type: none"> • Visma e-economic deletes data five years after the termination of the customer relationship, in accordance with the Danish Bookkeeping Act. 	<p>Deloitte has checked by way of inspection that the existing procedures for storage and deletion include specific requirements for the data processor's storage periods and deletion routines.</p> <p>Deloitte has inquired with relevant personal that personal data be stored in accordance with the agreed storage periods.</p> <p>Deloitte has inquired with relevant personal that personal data be deleted in accordance with the agreed deletion routines.</p>	<p>As a provider of accounting software, e-economic is subject to the requirements set forth in the Danish Bookkeeping Act (Bogføringsloven), which includes the obligation to retain customer data for 5 years plus the remaining part of the financial year for a given transaction after the agreement has been terminated.</p> <p>This legal obligation prevents Deloitte from testing the operational effectiveness of the control related to data deletion, as the necessary conditions for such testing are not present during the assurance period.</p> <p>No exceptions noted.</p>
D.3	<p>Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been:</p> <ul style="list-style-type: none"> • Returned to the data controller; and/or • Deleted if this is not in conflict with other legislation. 	<p>Deloitte has checked by way of inspection that formalised procedures are in place for the deletion or return of data.</p> <p>Deloitte has checked by way of inspection that formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data.</p>	<p>Refer to D.2.</p> <p>No exceptions noted.</p>

Control objective E**Procedures and controls are complied with to ensure that the data processor will only store personal data in accordance with the agreement with the data controller.**

No.	e-economic's control activity	Test performed by Deloitte	Results of Deloitte's test
E.1	<p>Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the data controller.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Deloitte has checked by way of inspection that formalised procedures exist for only storing and processing personal data in accordance with the data processing agreements.</p> <p>Deloitte has checked by way of inspection that the procedures are up to date.</p> <p>Deloitte has checked by way of inspection of a sample of data processing sessions from the data processor's list of processing activities that documentation exists that data processing takes place in accordance with the data processing agreement.</p>	No exceptions noted.
E.2	Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller.	<p>Deloitte has checked by way of inspection that the data processor has a complete and updated list of processing activities stating localities, countries or regions.</p> <p>Deloitte has checked by way of inspection of a sample of data processing sessions from the data processor's list of processing activities that documentation exists that the processing of data, including the storage of personal data, takes place only in the localities stated in the data processing agreement – or otherwise as approved by the data controller.</p>	No exceptions noted.

Control objective F

Procedures and controls are complied with to ensure that only approved sub-processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.

No.	e-conomic's control activity	Test performed by Deloitte	Results of Deloitte's test
F.1	<p>Written procedures exist which include requirements for the data processor when using sub-processors, including requirements for data processing agreements and instructions.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Deloitte has checked by way of inspection that formalised procedures are in place for using sub-processors, including requirements for data processing agreements and instructions.</p> <p>Deloitte has checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
F.2	The data processor only uses sub-processors to process personal data that have been specifically or generally approved by the data controller.	<p>Deloitte has checked by way of inspection that the data processor has a complete and updated list of sub-processors used.</p> <p>Deloitte has checked by way of inspection of a sample of sub-processors from the data processor's list of sub-processors that documentation exists that the processing of data by the sub-processors is stated in the data processing agreements – or otherwise as approved by the data controller.</p>	No exceptions noted.
F.3	When changing the generally approved sub-processors used, the data controller is informed in time to enable such controller to raise objections and/or withdraw personal data from the data processor.	<p>Deloitte has checked by way of inspection that formalised procedures are in place for informing the data controller when changing the sub-processors used.</p> <p>Deloitte has inspected documentation that the data controller was informed when changing the sub-processors used throughout the assurance period.</p>	No exceptions noted.

Control objective F

Procedures and controls are complied with to ensure that only approved sub-processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.

No.	e-conomic's control activity	Test performed by Deloitte	Results of Deloitte's test
F.4	The data processor has subjected the sub-processors to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	Deloitte has checked by way of inspection for existence of signed data processing agreements with sub-processors used, which are stated on the data processor's list. Deloitte has checked by way of inspection of a sample of data processing agreements that they include the same requirements and obligations as are stipulated in the data processing agreements between the data controllers and the data processor.	No exceptions noted.
F.5	The data processor has a list of approved sub-processors disclosing: <ul style="list-style-type: none">• Name• Business Registration No.• Address• Description of the processing.	Deloitte has checked by way of inspection that the data processor has a complete and updated list of sub-processors used and approved. Deloitte has checked by way of inspection that, as a minimum, the list includes the required details about each sub-processor.	No exceptions noted.
F.6	Based on an updated risk assessment of each sub-processor and the activity taking place at such processor, the data processor regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity.	Deloitte has checked by way of inspection that formalised procedures are in place for following up on processing activities at sub-processors and compliance with the data processing agreements. Deloitte has checked by way of inspection of	No exceptions noted.

Control objective F

Procedures and controls are complied with to ensure that only approved sub-processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.

No.	e-conomic's control activity	Test performed by Deloitte	Results of Deloitte's test
		<p>documentation that each sub-processor and the current processing activity at such processor are subjected to a risk assessment.</p> <p>Deloitte has checked by way of inspection of documentation that technical and organisational measures, security of processing at the sub-processors used, third countries' bases of transfer and similar matters are appropriately followed up on.</p> <p>Deloitte has inquired relevant personnel about informing data controllers when performing follow-up at sub-processors.</p>	No exceptions noted.

Control objective G**Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.**

No.	e-conomic's control activity	Test performed by Deloitte	Results of Deloitte's test
G.1	<p>Written procedures exist which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Deloitte has checked by way of inspection that formalised procedures exist to ensure that personal data are only transferred to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.</p> <p>Deloitte has checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
G.2	The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.	<p>Deloitte has checked by way of inspection that the data processor has a complete and updated list of transfers of personal data to third countries or international organisations.</p> <p>Deloitte has checked by way of inspection of a sample of data transfers from the data processor's list of transfers that documentation exists that such transfers were arranged with the data controller in the data processing agreement or subsequently approved.</p>	No exceptions noted.

Control objective G**Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.**

No.	e-conomic's control activity	Test performed by Deloitte	Results of Deloitte's test
G.3	As part of the transfer of personal data to third countries or international organisations, the data processor assessed and documented the existence of a valid basis of transfer.	<p>Deloitte has checked by way of inspection that formalised procedures are in place for ensuring a valid basis of transfer.</p> <p>Deloitte has checked by way of inspection that procedures are up to date.</p> <p>Deloitte has checked by way of inspection of a sample of data transfers from the data processor's list of transfers that documentation exists of a valid basis of transfer in the data processing agreement with the data controller and that transfers have only taken place in so far as this was arranged with the data controller.</p>	No exceptions noted.

Control objective H

Procedures and controls are complied with to ensure that the data processor can assist the data controller in handing out, correcting, deleting, or restricting information on the processing of personal data to the data subject.

No.	e-economic's control activity	Test performed by Deloitte	Results of Deloitte's test
H.1	<p>Written procedures exist which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Deloitte has checked by way of inspection that formalised procedures are in place for the data processor's assistance to the data controller in relation to the rights of data subjects.</p> <p>Deloitte has checked by way of inspection that procedures are up to date and assessments are planned on an annual basis.</p>	No exceptions noted.
H.2	<p>The data processor has established procedures in so far as this was agreed that enable timely assistance to the data controller in handing out, correcting, deleting or restricting or providing information about the processing of personal data to data subjects.</p>	<p>Deloitte has checked by way of inspection that the procedures in place for assisting the data controller include detailed procedures for:</p> <ul style="list-style-type: none"> • Handing out data • Correcting data • Deleting data • Restricting the processing of personal data • Providing information about the processing of personal data to data subjects. <p>Deloitte has checked by way of inspection of documentation that the systems and data-bases used support the performance of the relevant detailed procedures.</p>	No exceptions noted.

Control objective I

Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into.

No.	e-economic's control activity	Test performed by Deloitte	Results of Deloitte's test
I.1	<p>Written procedures exist which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Deloitte has checked by way of inspection that formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches.</p> <p>Deloitte has checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
I.2	<p>Visma e-economic has established controls to identify any personal data breaches, including:</p> <ul style="list-style-type: none"> • Awareness of employees • Monitoring of network traffic • Log monitoring 	<p>Deloitte has checked by way of inspection that the data processor provides awareness training to the employees in identifying any personal data breaches.</p> <p>Deloitte has checked by way of inspection of documentation that network traffic is monitored and that anomalies, monitoring alarms, large file transfers, etc. are followed up on.</p> <p>Deloitte has checked by way of inspection of documentation that logging of access to personal data, including follow-up on repeated attempts to gain access, is followed up on a timely basis.</p>	No exceptions noted.
I.3	<p>If any personal data breach occurred, the data processor informed the data controller without undue delay after having become aware of such personal data breach at the data processor or a sub-processor.</p>	<p>Deloitte has checked by way of inspection that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach.</p> <p>Deloitte has made inquiries of the sub-processors as to whether they have identified any personal data breaches throughout the assurance period.</p>	No exceptions noted.

Control objective I

Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into.

No.	e-conomic's control activity	Test performed by Deloitte	Results of Deloitte's test
		<p>Deloitte has checked by way of inspection that the data processor has included any personal data breaches at sub-processors in the data processor's list of security incidents.</p> <p>Deloitte has checked by way of inspection that a sample of personal data breaches recorded at the data processor or the sub-processors have been communicated to the data controllers concerned without undue delay after the data processor became aware of the personal data breaches.</p>	
I.4	The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency.	<p>Deloitte has checked by way of inspection that the procedures in place for informing the data controllers in the event of any personal data breach include detailed procedures for describing:</p> <ul style="list-style-type: none"> • The nature of the personal data breach; • The probable consequences of the personal data breach; • Measures taken or proposed to be taken to respond to the personal data breach. <p>Deloitte has checked by way of inspection of documentation that the procedures available support that measures are taken to respond to the personal data breach.</p>	No exceptions noted.

PENNEO

The signatures in this document are legally binding. The document is signed using Penneo™ secure digital signature. The identity of the signers has been recorded, and are listed below.

“By my signature I confirm all dates and content in this document.”

Karina Wellendorph

Intern underskriver

Serial number: c0950e89-7780-4ce9-8c0f-d09cb1e277b6

IP: 93.165.xxx.xxx

2026-02-04 14:03:51 UTC



Thomas Kühn

DELOITTE STATS AUTORISERET REVISIONSPARTNERSELSKAB

CVR: 33963556

Ekstern underskriver

Serial number: 980d9b01-fe6c-4607-ace3-663c843ac5b0

IP: 163.116.xxx.xxx

2026-02-05 08:11:52 UTC



Penneo document key: VV0LO-5QPWR-MD8DP-F2JLI-SV2KF-IYHJR

This document is digitally signed using [Penneo.com](https://penneo.com). The signed data are validated by the computed hash value of the original document. All cryptographic evidence is embedded within this PDF for future validation.

The document is sealed with a Qualified Electronic Seal. For more information about Penneo's Qualified Trust Services, visit <https://eutl.penneo.com>.

How to verify the integrity of this document

When you open the document in Adobe Reader, you should see that the document is certified by **Penneo A/S**. This proves that the contents of the document have not been modified since the time of signing. Evidence of the individual signers' digital signatures is attached to the document.

You can verify the cryptographic evidence using the Penneo validator, <https://penneo.com/validator>, or other signature validation tools.