



**Table of contents**

- 1. Independent auditor’s report .....1**
- 2. Management assertion .....4**
- 3. Description of processing .....6**
- 4. Visma e-conomic’s control objectives, controls, test and results.....13**

## **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 "Visma e-conomic") description in section 3 of the described services in accordance with the data processing agreements with customers as of November 9, 2021 (hereinafter "the description"), and about the design and implementation of controls related to the control objectives stated in the description.

Visma uses the following sub-data processors Google Cloud Platform, Amazon Web Services, Microsoft Azure, Twilio, Actito and 84codes. Visma 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-data processors.

Some of the control objectives described in Visma 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 Visma e-conomic. The opinion does not include the suitability of the design and operating effectiveness of these complementary controls.

#### **Visma e-conomic's responsibilities**

Visma 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 and implementing controls to achieve the stated control objectives.

#### **Auditor's independence and quality control**

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

We are subject to the International Standard on Quality Control (ISQC 1) and accordingly use and maintain a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

#### **Auditor's responsibilities**

Our responsibility is to express an opinion on Visma e-conomic's description and on the design and implementation 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 Visma e-conomic's

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

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 Visma e-conomic**

Visma 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 as of November 9, 2021; and
- (b) The controls related to the control objectives stated in the description were suitably designed as of November 9, 2021.

### **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 Visma 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, December 22, 2021

### **Deloitte**

Statsautoriseret Revisionspartnerselskab  
CVR No. 33 96 35 56



Thomas Kühn  
Partner, State-Authorised Public Accountant



Halik Canitez  
Senior Manager

## 2. Management assertion

The accompanying description has been prepared for Visma's 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.

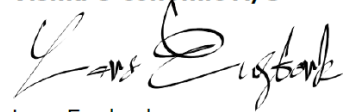
Visma e-economic confirms that:

- a) The accompanying description in section 3 fairly presents Visma e-economic's application (e-economic), which has processed personal data for data controllers covered by the General Data Protection Regulation as of November 9, 2021. 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 as of November 9, 2021.
  - (iii) Does not omit or distort information relevant to the scope of Visma's e-economic application being (e-economic) 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 as of November 9, 2021. 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.
- 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, December 22, 2021

**Visma e-conomic A/S**



Lars Engbork  
Managing Director

### **3. Description of processing**

#### **1. About Visma e-economic**

Visma e-economic A/S is a software company selling cloud-based solutions within the areas of ERP, electronic invoicing and accounting to the Danish market.

Visma e-economic is owned by Visma - a leading provider of core business software for a more efficient and resilient society and headquartered in Norway. Visma simplifies the work of companies and organisations of all sizes, empowering people and helping businesses grow and thrive. Visma has more than 13,600 employees and 1 million customers across the Nordics, Benelux, Central and Eastern Europe and Latin America who share the same passion to **make progress happen**.

By taking advantage of opportunities in a fast-moving market characterised by rapid development in technology, Visma has turned into an international leader in cloud software delivery and cloud solutions are Visma's top priority.

As a provider of mission critical systems, Visma takes great responsibility when it comes to information security and protecting the privacy of its customers and employees, and therefore, Visma is continuously working on improving its security and data protection procedures and practices throughout the organisation.

#### **2. Organisation of Data Protection**

##### **2.1 Data protection in Visma e-economic**

Visma e-economic has a dedicated Legal & Compliance team whose responsibility is to ensure compliance with all relevant data protection laws and regulations, including the General Data Protection Regulation (GDPR). The team oversees data security strategy, GDPR compliance, as well as other legal areas to support customers and employees.

##### **2.2 Data Protection Officer**

Visma has appointed a Data Protection Officer (DPO) to oversee data protection at the group level. The DPO is an appointed Visma employee with a dedicated role description to facilitate the privacy work within Visma. The DPO is registered at all national data protection authorities where Visma operates.

##### **2.3 Data Protection Council**

All strategic decisions regarding privacy are made and governed by Visma's Data Protection Council in order to ensure transparency and accountability. The Council consists of the DPO, CISO, selected Data Protection Managers, and some of the legal counsels in Visma.

##### **2.4 Data Protection Managers**

A Data Protection Manager (DPM) is an appointed employee in all Visma companies, who has a dedicated role description for their role as DPM. The DPM continuously reports to and works together with the DPO to solve everyday tasks in their respective business units. In addition, all DPMs report directly to the Council on a variety of issues to ensure progress on all of Visma's strategic efforts related to privacy.

In Visma e-economic the appointed DPM is the Head of Legal & Compliance, who is also part of the Data Protection Council.

##### **2.5 Each employee**

Each Visma employee is responsible for abiding by and supporting the Visma Privacy Framework in his or her daily work. The individual employee's contribution is essential in order for Visma to succeed in its



effort to ensure data protection and privacy. Employees in Visma e-economic are informed of this upon onboarding and reminded of this on an ongoing basis through various internal GDPR awareness campaigns.

### **3. Scope of audit**

This audit is focused on *e-economic*, the accounting software developed and sold by Visma e-economic in Denmark. For the scope of this audit, Visma e-economic is audited in its role as data processor.

#### **3.1 Description of processing**

Visma e-economic processes personal data on behalf of its customers, who act as data controllers of the data that they process within e-economic. Processing personal data on behalf of the data controller is based on an agreement between Visma e-economic and the customer. The data processing agreement is included in Appendix 1 to Visma e-economic's "Abonnementsvilkår for e-economic" which can be found on Visma e-economic's [website](#) and within the e-economic application.

The purpose in which Visma e-economic processes its customers' data is to ensure the data controller's use of the e-economic application and the fulfilment of the data processing agreement.

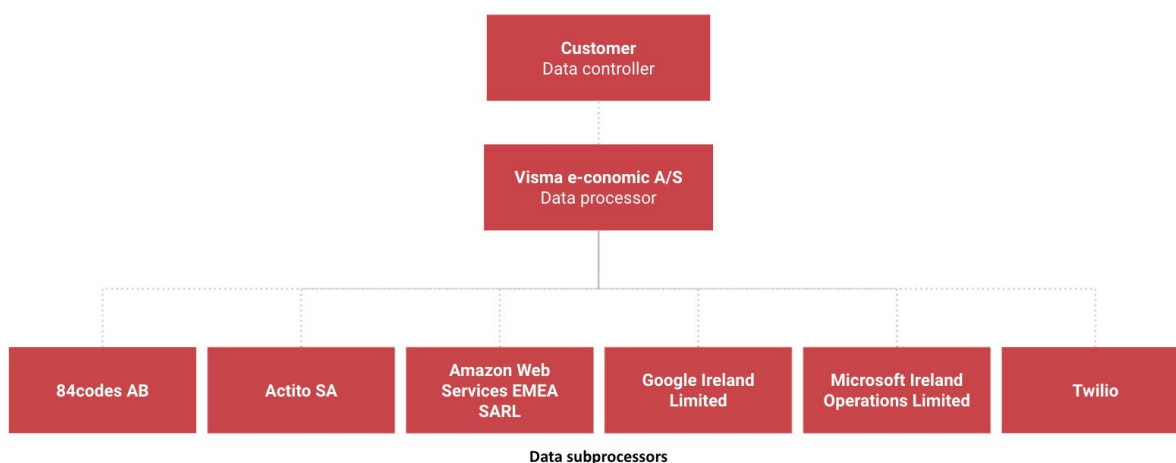
#### **3.2 e-economic application description**

e-economic is a cloud-based accounting system, developed and offered by Visma e-economic which enables small and medium-sized businesses to operate their accounting and bookkeeping practices as expected by 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. Furthermore, it is possible to upscale the system to have ERP functionalities. In e-economic, customers can handle invoicing, sales, finance, bookkeeping, VAT accounts and the statement, reporting, etc. In connection with these services, personal information is included, which Visma e-economic processes on behalf of the customer.

Visma e-economic processes all personal data added to the e-economic application in its role as data processor.

#### **3.3 Data sub-processors**

A reference to sub-processors that Visma e-economic engages with is found within the data processing agreement entered into with customers. The agreement states that the customers have given their general consent for Visma e-economic to change or engage with additional sub-processors. Prior to engaging with new sub-processors, Visma e-economic will ensure to inform its customers in advance.



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

Sub-processor	Purpose
84codes AB	84codes is a queuing system that is used when customers send an email or invoice through e-economic. In addition, 84codes allows different parts of the application to communicate with each other.
Actito SA	MessageCloud by SmartFocus supports the sending of emails generated through the e-economic application.
Amazon Web Services EMEA SARL	Amazon hosts attachments and images for postings in 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 Visma e-economic's database backup.
Twilio	SendGrid supports sending emails and invoices generated through the e-economic application.

### 3.4 The nature of processing

In general, Visma e-economic processes general categories of personal data such as name, job title, e-mail, phone number and CPR number.

However, Visma e-economic does not control which categories of personal data are added to e-economic. Therefore, the categories of data processed by each customer varies from agreement to agreement. It is thus possible that a customer may process sensitive data, such as data related to health, sexual orientation and trade union membership, within e-economic.

Additionally, Visma e-economic 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 (including employees and/or contact persons)
- Data controller's suppliers.

Depending on how customers use e-economic, Visma e-economic may also process other categories of data subjects.

### 3.5 Risk assessment

Visma e-economic 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, Visma e-economic uses the risk = impact x likelihood methodology, with risk, impact and likelihood levels appropriate to Visma e-economic 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, Visma e-economic is able to maintain an acceptable level of risk through the implementation of technical and organisational controls.

Risk management at Visma e-economic is implemented on multiple levels. On a high level, the Security Forum in Visma e-economic 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 prioritised for elimination and mitigation at the forum.

A risk-based security assessment of the e-economic application and its components is performed on an annual basis and is reviewed and approved by Visma Group Security and Visma Group Privacy. The purpose is to provide documentation of how e-economic fulfils certain requirements and recommendations for application security, information security and privacy/data protection as well as actions that must or should be taken in order to improve security and compliance. Actions to be taken are generated as tickets, which are prioritised based on risk to customers and Visma e-economic.

Visma e-economic also performs a privacy risk assessment annually in regard to the processing of its customer's personal data. The assessment considers the likelihood and impact of the loss of confidentiality, integrity and availability of personal data for the data subjects and Visma e-economic. The purpose of this assessment is to evaluate whether the technical and organisational controls in place are sufficient to protect the data processed.

For all third-parties that process personal data on behalf of Visma e-economic and its customers, vendor risk assessments are performed annually. These assessments consider the types and amount of personal data processed by third-parties and the controls in place to protect the data, e.g. where data is hosted, level of encryption and deletion procedures. For third-parties that process data outside of the EU/EEA, risks are created for the processing of data in third countries. In response, Visma e-economic performs a Transfer Impact Assessment to evaluate the level of security and privacy in the relevant countries where data is processed.

### 3.6 Control measures

Visma e-economic 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-data 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 Visma 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.

### 3.6.1 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.

Visma e-conomic has prepared several procedures which describe how personal data is to be processed in order to ensure a 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. New employees are furthermore 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 Visma e-conomic enters into with customers.

### 3.6.2 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, Visma 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 Visma 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, Visma 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 procedure for testing and quality assurance procedures, monitoring logs and updating software as needed.

### 3.6.3 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, Visma e-conomic 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, Visma e-conomic maintains a common Group-wide Information Security Policy. This Information Security Policy is updated annually and is available to all employees in Visma e-conomic's intranet.

Prior to employment, Visma e-conomic 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 Information Security Policy before their first day.

All new employees participate in an onboarding session where the 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 Visma e-conomic enters with customers. Visma e-conomic has a dedicated Legal & Compliance team that supports the rest of the organisation with questions related to GDPR. When employees terminate at Visma e-conomic, they are once again reminded of their duty of confidentiality in a written letter that they must sign.

#### 3.6.4 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.

Visma e-economic has procedures in place for deletion of personal data. Upon active termination of a customer's agreement, Visma e-economic will set all customer-owned data for deletion. If the e-economic agreement has been terminated actively by the customer, customer-owned data will be set for deletion in the production database 180 days following the termination date. This also applies to trial agreements.

If the agreement has been terminated due to non-payment, customer-owned data will be set for deletion in the production database after 360 days following termination date.

While the agreement is still active, customers of Visma e-economic are given the option to delete and anonymise their personal data themselves. At all times, customers can delete other users in the agreement, who may no longer need access to their accounting data or have a legitimate purpose to do so. Furthermore, customers are able to anonymise the data on their customers that they process. The reason why it is not possible for customers to *delete* data on their customers is because deleting data would cause the e-economic application to miscalculate the balances of customers.

#### 3.6.5 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.

Visma e-economic has procedures in place for storage of personal data. Visma e-economic retains personal data as long as a customer relationship exists. Employees of Visma e-economic have been informed about how to process personal data in accordance with the data processing agreement entered into with customers.

#### 3.6.6 Use of sub-data processors (control objective F)

Procedures and controls are complied with to ensure that only approved sub-data processors are used and that, when following up on such sub-data processors' 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 have given their general consent for Visma e-economic to change or engage with sub-data processors. Visma e-economic updates and maintains a full overview of sub-data processors, which is available on Visma e-economic's website. Visma e-economic has data processing agreements in place with all sub-data processors and makes sure that sub-data processors are subject to the same conditions and requirements as set forth in the data processing agreement that Visma e-economic has with customers. Finally, Visma e-economic regularly monitors, reviews and audits all sub-data processors through questionnaires and/or gathering and reviewing of auditor's reports.

#### 3.6.7 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.

Visma e-economic 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 customers. When transferring personal data to a third country, Visma e-economic ensures to implement an appropriate legal transfer mechanism such as, e.g., implementing EU SCC and performing a Transfer Impact Assessment to evaluate the level of security and privacy in the relevant countries where data is processed.

Visma e-economic is aware that the Privacy Shield has been declared invalid and that transfer of personal data to a third country therefore requires a different legal transfer mechanism. Transfer of data to a third country (including the Schrems II case) is an area that Visma e-economic pays a lot of attention to. Visma e-economic awaits further guidance and best practice to handle this issue. This might include implementation of further measures and changes to existing agreements with data processors.

#### 3.6.8 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.

Visma e-economic 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.

#### 3.6.9 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.

Visma e-economic has prepared procedures for handling potential and actual security breaches. All employees have been made aware of these procedures, as they have a role to play in reporting security incidents. In addition, Visma e-economic has set up a Crisis Communication team dedicated to ensuring that communication to customers regarding incidents happens in accordance with the data processing agreement and in the best way possible.

Upon request, Visma e-economic will assist its customers by providing relevant information when it is deemed necessary to notify the Data Protection Authorities.

#### 3.6.10 Complementary data controller controls

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

Customers of Visma 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-economic's control objectives, controls, test and results

### Introduction

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

Our testing of Visma e-economic'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, Visma e-economic'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 Visma e-economic.
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.

<b>Control objective A</b>			
<b>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.</b>			
<b>No.</b>	<b>Visma e-conomic's control activity</b>	<b>Test performed by Deloitte</b>	<b>Results of Deloitte's test</b>
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 is 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-conomic 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 checked by way of inspection of a sample of one data processing operation that these are conducted consistently with instructions.</p>	No exceptions noted.
A.3	<p>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.</p>	<p>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>	No exceptions noted.



**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.**

<b>No.</b>	<b>Visma e-conomic's control activity</b>	<b>Test performed by Deloitte</b>	<b>Results of Deloitte's test</b>
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.**

<b>No.</b>	<b>Visma e-conomic's control activity</b>	<b>Test performed by Deloitte</b>	<b>Results of Deloitte's test</b>
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 of a sample of one data processing agreement that the safeguards agreed have been established.</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.	Visma 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 network diagrams and other network documentation to ensure appropriate 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.**

<b>No.</b>	<b>Visma e-conomic's control activity</b>	<b>Test performed by Deloitte</b>	<b>Results of Deloitte's test</b>
		<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 one 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 one alarm, 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.**

<b>No.</b>	<b>Visma e-conomic's control activity</b>	<b>Test performed by Deloitte</b>	<b>Results of Deloitte's test</b>
		<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"><li>• Activities performed by system administrators and others holding special rights;</li><li>• Security incidents comprising:<ul style="list-style-type: none"><li>○ Changes in log set-ups, including disabling of logging;</li><li>○ Changes in users' system rights;</li><li>○ Failed attempts to log on to systems, databases or networks;</li></ul></li></ul> <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 one day 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.**

<b>No.</b>	<b>Visma e-conomic's control activity</b>	<b>Test performed by Deloitte</b>	<b>Results of Deloitte's test</b>
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 one development or test database that personal data included therein is pseudonymised or anonymised.</p> <p>Deloitte has checked by way of inspection of a sample of one development or test database in which personal data is 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.**

<b>No.</b>	<b>Visma e-conomic's control activity</b>	<b>Test performed by Deloitte</b>	<b>Results of Deloitte's test</b>
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 one employee's access to systems and databases that the user 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 one 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.**

<b>No.</b>	<b>Visma e-conomic's control activity</b>	<b>Test performed by Deloitte</b>	<b>Results of Deloitte's test</b>
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 is 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 is 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 is 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.**

<b>No.</b>	<b>Visma e-conomic's control activity</b>	<b>Test performed by Deloitte</b>	<b>Results of Deloitte's test</b>
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 past year.</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 one data processing agreement that the requirements in this agreement is 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> <p>Assessment of CV.</p>	<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 one employee appointed during the assurance period that documentation exists of the screening having comprised:</p> <ul style="list-style-type: none"><li>• Assessment of CV.</li></ul>	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.	Visma e-conomic'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 one employee appointed during the assurance period that the relevant employees have signed a confidentiality agreement.</p> <p>Deloitte has checked by way of inspection of one employee appointed during the assurance period that the relevant employees have been introduced to:</p> <ul style="list-style-type: none"> <li>• Information security policy;</li> <li>• Procedures for processing data and other relevant information.</li> </ul>	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, including 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 one employee 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 one employee resigned or dismissed during</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.**

<b>No.</b>	<b>Visma e-conomic's control activity</b>	<b>Test performed by Deloitte</b>	<b>Results of Deloitte's test</b>
		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 all 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.**

<b>No.</b>	<b>Visma e-conomic's control activity</b>	<b>Test performed by Deloitte</b>	<b>Results of Deloitte's test</b>
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"><li>• Visma e-conomic deletes data in the event of termination of a customer relationship.</li></ul>	<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 checked by way of inspection of a sample of one data processing session from the data processor's list of processing activities that documentation exists that personal data are stored in accordance with the agreed storage periods.</p> <p>Deloitte has checked by way of inspection of a sample of one data processing session from the data processor's list of processing activities that documentation exists that personal data is deleted in accordance with the agreed deletion routines.</p>	No exceptions noted.
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"><li>• Returned to the data controller; and/or</li><li>• Deleted if this is not in conflict with other legislation.</li></ul>	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.	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.**

<b>No.</b>	<b>Visma e-conomic's control activity</b>	<b>Test performed by Deloitte</b>	<b>Results of Deloitte's test</b>
		Deloitte has checked by way of inspection of one terminated data processing session during the assurance period that documentation exists that the agreed deletion or return of data has taken place.	

**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.**

<b>No.</b>	<b>Visma e-conomic's control activity</b>	<b>Test performed by Deloitte</b>	<b>Results of Deloitte's test</b>
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 one data processing session 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 one data processing session 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-data 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.**

<b>No.</b>	<b>Visma e-conomic's control activity</b>	<b>Test performed by Deloitte</b>	<b>Results of Deloitte's test</b>
F.1	<p>Written procedures exist which include requirements for the data processor when using sub-data processors, including requirements for sub-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-data processors, including requirements for sub-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	<p>The data processor only uses sub-data processors to process personal data that have been specifically or generally approved by the data controller.</p>	<p>Deloitte has checked by way of inspection that the data processor has a complete and updated list of sub-data processors used.</p> <p>Deloitte has checked by way of inspection of a sample of one sub-data processor from the data processor's list of sub-data processors that documentation exists that the processing of data by the sub-data processor is stated in the data processing agreements – 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-data 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.**

<b>No.</b>	<b>Visma e-conomic's control activity</b>	<b>Test performed by Deloitte</b>	<b>Results of Deloitte's test</b>
F.3	When changing the generally approved sub-data 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. When changing the specially approved sub-data processors used, this has been approved by the data controller.	Deloitte has checked by way of inspection that formalised procedures are in place for informing the data controller when changing the sub-data processors used.  Deloitte has inspected documentation that the data controller was informed when changing the sub-data processors used throughout the assurance period.	No exceptions noted.
F.4	The data processor has subjected the sub-data processor 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 sub-data processing agreements with sub-data processors used, which are stated on the data processor's list.  Deloitte has checked by way of inspection of a sample of one sub-data processing agreement 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-data processors disclosing: <ul style="list-style-type: none"><li>• Name</li><li>• Business Registration No.</li><li>• Address</li><li>• Description of the processing.</li></ul>	Deloitte has checked by way of inspection that the data processor has a complete and updated list of sub-data processors used and approved.  Deloitte has checked by way of inspection that, as a minimum, the list includes the required details about each sub-data processor.	No exceptions noted.



**Control objective F**

**Procedures and controls are complied with to ensure that only approved sub-data 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.**

<b>No.</b>	<b>Visma e-conomic's control activity</b>	<b>Test performed by Deloitte</b>	<b>Results of Deloitte's test</b>
F.6	Based on an updated risk assessment of each sub-data 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. The data controller is informed of the follow-up performed at the sub-data processors, if relevant.	<p>Deloitte has checked by way of inspection that formalised procedures are in place for following up on processing activities at sub-data processors and compliance with the sub-data processing agreements.</p> <p>Deloitte has checked by way of inspection of documentation that each sub-data 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-data 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-data 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.**

<b>No.</b>	<b>Visma e-conomic's control activity</b>	<b>Test performed by Deloitte</b>	<b>Results of Deloitte's test</b>
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 is 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>	<p>Visma e-conomic uses sub-data processors where new measures should be implemented to comply with GDPR after the Schrems II ruling. Please refer to management's description in section 3 regarding transfer of personal data to third countries.</p> <p>No exceptions noted.</p>
G.2	<p>The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.</p>	<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 one data transfer 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>	<p>Refer to G.1.</p> <p>No exceptions noted.</p>

**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.**

<b>No.</b>	<b>Visma e-conomic's control activity</b>	<b>Test performed by Deloitte</b>	<b>Results of Deloitte's test</b>
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 one 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>	<p>Refer to G.1.</p> <p>No exceptions noted.</p>

**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.**

<b>No.</b>	<b>Visma e-conomic's control activity</b>	<b>Test performed by Deloitte</b>	<b>Results of Deloitte's test</b>
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.</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"><li>• Handing out data</li><li>• Correcting data</li><li>• Deleting data</li><li>• Restricting the processing of personal data</li><li>• Providing information about the processing of personal data to data subjects.</li></ul> <p>Deloitte has checked by way of inspection of documentation that the systems and databases 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.**

<b>No.</b>	<b>Visma e-conomic's control activity</b>	<b>Test performed by Deloitte</b>	<b>Results of Deloitte's test</b>
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. Deloitte has checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
I.2	<p>Visma e-conomic has established controls to identify any personal data breaches, including:</p> <ul style="list-style-type: none"><li>• Awareness of employees</li><li>• Monitoring of network traffic</li><li>• Log monitoring.</li></ul>	<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-data 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-data 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.**

<b>No.</b>	<b>Visma e-economic's control activity</b>	<b>Test performed by Deloitte</b>	<b>Results of Deloitte's test</b>
		<p>Deloitte has checked by way of inspection that the data processor has included any personal data breaches at sub-data processors in the data processor's list of security incidents.</p> <p>Deloitte has checked by way of inspection that all personal data breaches recorded at the data processor or the sub-data processors have been communicated to the data controllers concerned without undue delay after the data processor became aware of the personal data breach.</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"><li>• The nature of the personal data breach;</li><li>• The probable consequences of the personal data breach;</li><li>• Measures taken or proposed to be taken to respond to the personal data breach.</li></ul> <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.