



# revi-it

Building a safer society through compliance

## Assurance report

# ag analytics a/s

Independent auditor's ISAE 3000 assurance report with limited security on information security and measures pursuant to the data processing agreements with customers, who have used Autoflows as of 11 February 2022.

February 2022

REVI-IT A/S | [www.revi-it.dk](http://www.revi-it.dk)  
Højbro Plads 10, 1200 København K  
CVR: 30 98 85 31 | Tel. 33 11 81 00 | [info@revi-it.dk](mailto:info@revi-it.dk)  
[www.dpo-danmark.dk](http://www.dpo-danmark.dk) | [www.revi-cert.dk](http://www.revi-cert.dk)

## Table of contents

Section 1:	ag analytics a/s' description of processing activity for the supply of Autoflows .....	1
Section 2:	ag analytics a/s' statement.....	6
Section 3:	Independent auditor's ISAE 3000 assurance report with limited assurance on information security and measures pursuant to data processing agreements with customers who has used Autoflows as per 11 February 2022 .....	8
Section 4:	Control objectives, controls, tests, and results hereof.....	11

**Disclaimer:**

The English version of this report was translated for the convenience of the reader. This translation has not been reviewed or approved by REVI-IT A/S' auditors. In all legal matters, please refer to the Danish version.

## Section 1: ag analytics a/s' description of processing activity for the supply of Autoflows

The purpose of this description is to provide information for ag analytic a/s' customers and their stakeholders (including auditors) of compliance with the contents of EU's General Data Protection Regulation ("GDPR").

Further, the purpose of this description, is to provide specific information of questions regarding processing security, technical and organizational measures, responsibilities between data controller (our customers) and the processor (ag analytics a/s) and how the services offered can assist in supporting the data subjects' rights.

### Our control objectives, including rules and procedures and also implemented controls

#### ag analytics a/s and Autoflows

ag analytics a/s is a SaaS (Software as a Service) company, assisting car dealers and workshops with improving their performance and customer satisfaction. We have worked with the auto business for more than 10 years and our CEM system is used by more than 380 car dealers and workshops all over the Nordic countries.

Autoflows is the name of our service provided to the car business and is a complete and ready to go solution, without set-up, assisting dealers and workshops automate manual and time-consuming tasks, such as calling in customers for service check, wheel change or customer satisfaction. Autoflows makes it easy for the customers to book online, providing the workshops with a constant flow of customers and increased earnings.

### Principles regarding processing of personal data

ag analytics a/s is processing data on behalf of our Autoflows users. The users are data controllers.

ag analytics a/s has the following general guidelines:

- Information security policy
- Employee guidelines
- Privacy policy

The guidelines state how ag analytics a/s relates to the processing of personal data. To help us control the processing of personal data, we have the following procedures, which also include corresponding controls:

- Access control
- Acquisition and development
- Personal data request management
- Security incidents management
- Contract management
- Risk management

## Risk management within ag analytics a/s

ag analytics a/s has a procedure for risk management, in which we relate to the procedures, established to safeguard our operations and the control of same. ag analytics a/s will hold weekly team meetings, where control of procedures is included and also issues such as e.g., logging, chain of events and other things relevant to the company's risk management.

## Risk analysis - ag analytics a/s

<b>The processing of data is characterized by:</b>	No	Yes
Large number of data		x
Long term processing	x	
Many users	x	
Significant dependency of organisational security / that processes, and agreements are followed manually	x	
Sensitive data, criminal records and/or CPR-numbers	x	
Data processor / sub-data processor		x
Authorised transfer of data to third countries		x
Data subjects with special needs for protection	x	
New technologies	x	
Systematic and extensive assessment of private data, based on automated processing, including profiling which produces legal effects concerning the data subject or similarly significantly affects the data subject.	x	
Large number of sensitive data or criminal convictions.	x	
Systematic large scale monitoring of a publicly accessible area	x	

## Organisation and responsibility

ag analytics a/s employs around 20 full-time and part-time employees, organized as follows:

- Board of directors
- Management consisting of CEO, CTO and COO
- Commercial teams
- Data Science team
- Support team

Management has the overall responsibility to make sure, that all procedures are followed and updated when needed. Weekly meetings are being held in all teams, where communication and information about procedures and incidents are being discussed.

## GDPR and ag analytics a/s' roles and responsibilities in the role of data processor

ag analytics a/s is a Software as a Service company, developing software, made available to our users. Ag analytics processes data on behalf of the data controllers (our users). According to our data processing agreement, we only process personal data according to documented instructions from the data controller (our users) and we immediately inform the data controller, if instructions in the data processor's (ag analytics a/s) opinion is evaluated to be in violation of general data protection regulation or data protection regulations in other EU-law or Member States' national law.

ag analytics a/s has established procedures for access control, to ensure that only persons actually authorised for this, has access to the personal data, processed on behalf of the data controller (the workshop). Moreover, ag analytics a/s ensures that the persons authorised to process personal data on behalf of the data controller (the workshop) have committed themselves to confidentiality or are subjected to a suitable legal obligation of secrecy.

### Consent

ag analytics a/s does not obtain consent, which is in the hands of the data controller (the dealers and the workshops). ag analytics a/s can in certain cases (where the workshops own system-integrations allow it) assist with gathering and renewal of consent on behalf of the workshop.

### Processing of difference categories of personal data

ag analytics a/s is data processor on behalf of our users, which are data controllers. In our privacy policy we describe the data vi process as: general personal data, sensitive personal data and personal data containing offences and criminal convictions:

1. General personal data:
  - Name
  - Address
  - CVR-number
  - E-mail address
  - Telephone number
2. Sensitive personal data
  - None
3. Details about offences and criminal convictions
  - None

There are procedures for requests about personal data, for incidents concerning personal data, and also guidelines for employees with access to personal data in connection with development or administration of our services. The procedures are linked to a number of controls, performed on a regular basis and when needed, according to our annual wheel.

### Rights of the data subject

ag analytics a/s has described its obligations to our registered users and their customers, in a data processing agreement and is subject to this, as well as current legislation. Procedures and controls have been established of how we manage personal data requests.

## General obligations in the role of data processor

Upon signing the contract, our users will receive a data processing agreement, describing their' and our obligations as data controller respectively data processor. ag analytics a/s has established procedures ensuring our obligations as data processor, including making sure that we do not sign contracts or agreements that can lead to security breaches and violation of current legislation. Likewise, procedures and controls have been established as to how we monitor our sub-suppliers.

ag analytics a/s is responsible – through the signing of a data processing agreement – for subjecting a possible sub-data processor at the very least, to the obligations the data processor himself is subjected to, according to the data protection law.

## Data protection officer (DPO)

ag analytics a/s has appointed a DPO as of 1 September 2021. The DPO has been selected, based on the Danish Data Protection Agency's guidelines. The DPO refers to ag analytics a/s' CEO and works with company risk management, based on the existing annual wheel.

## Transfer of personal data

ag analytics a/s has procedures for access control and guidelines for employees, ensuring proper processing of personal data.

According to our data processing agreement, we only process personal data based on documented instructions from the data controller, including transfer (making available, disclosure, including internal use) of personal data to third countries or international organisations.

Our users and their customers can at any time, contact us concerning their data, after which ag analytics a/s' procedures for personal data requests become effective.

## Security of processing, notification, and communication

ag analytics a/s has an information security policy, providing the setting for the organisational and technical guidelines for the company. We operate, based on a number of procedures related to the processing of personal data.

Procedures have been established and are being followed within the following areas:

- Access management
- Acquisition and development
- Personal data request management
- Security incidents management
- Contract management
- Risk management

We have specific working procedures related to processing and requests regarding personal data. Requests are registered in a daily status mail from Support, who handles requests. Subsequently an anonymized log of requests is being kept, enabling management to monitor, whether requests are being managed according to procedures. The daily status from Support states the nature of the request and the solution hereof.

## Full transparency for data controllers and data subjects

ag analytics a/s' employees are informed about their role as data controllers and especially our Data Science team, developing and testing our solutions, are following procedures about development, including secure handling of personal data in test environments.

All our users and their customers can, at any given time, contact us about their personal data, after which the procedure for personal data requests become effective.

## Privacy by design and by default

ag analytics a/s establish, as standard, privacy by design when developing our solutions for workshops and dealers and for our overall administrative procedures. We have a procedure for acquisition and development, which relates to for instance test environment, commencement of operations and approvals to secure personal data.

## Compliance

ag analytics a/s has described and prepared a number of procedures, based on The General Data Protection Regulation's criteria for security. The procedures' controls are performed on a regular basis and when needed, relatively to the risk. The different teams in ag analytics a/s will hold weekly meetings. Weekly meetings are being held by management and the Board of Directors hold quarterly meetings. The structure of the meetings and the size of the company allow a good communications flow and swift handling of potential critical incidents.

Once a year, in connection with the annual audit, the Board of Directors will address compliance.



## Section 2: ag analytics a/s' statement

The accompanying description has been prepared for ag analytics a/s customers, who have signed a data processing agreement with ag analytics a/s in connection with supply of the service Autoflows, and who has a sufficient understanding to consider the description along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the EU Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter “the Regulation”) have been complied with.

ag analytics a/s uses the sub-suppliers and sup-processors Host Europe, Alchemer, MailChimp, ScanNet, IT Arkitekterne, Olinecity.io, TMPO and Google Cloud. This statement does not include control objectives and related controls at ag analytics a/s' sub-suppliers and sub-processors.

ag analytics a/s confirms that:

- a) The accompanying description, Section 1, fairly presents how ag analytics a/s has processed personal data on behalf of data controllers subject to the Regulation per 11 February 2022. The criteria used in making this statement were that the accompanying description:
  - (i) Presents how ag analytics a/s' processes and controls related to data protection were designed and implemented, including:
    - The types of services provided, including the type of personal data processed
    - The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete, and restrict processing of personal data
    - The procedures used to ensure that data processing has taken place in accordance with contract, instructions, or agreement with the data controller
    - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality
    - The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation
    - The procedures supporting in the event of breach of personal data security that the data controller may report this to the supervisory authority and inform the data subjects
    - The procedures ensuring appropriate technical and organisational safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed
    - Controls that we, in reference to the scope of ag analytics a/s have assumed would be implemented by the data controllers and which, if necessary, in order to achieve the control objectives stated in the description, are identified in the description
    - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the processing of personal data



- (ii) Includes relevant information about changes in the Data Processor's supply of Autoflows for processing of personal data, undertaken per 11 February 2022.
  - (iii) Does not omit or distort information relevant to the scope of Autoflows for processing of personal data while acknowledging that the description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of Autoflows that the individual data controllers might consider important in their particular circumstances.
- b) The controls related to the control objectives stated in the accompanying description were, in our view, suitably designed and implemented per 11 February 2022. 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; and
  - (ii) The identified controls would, if implemented as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.
- c) Appropriate technical and organisational safeguards were established and maintained to comply with the agreements with the data controllers, sound data processing practices and relevant requirements for data processors in accordance with the Regulation.

Copenhagen, 21 February 2022  
ag analytics a/s

Nicholas Malcolm  
Managing Director & Partner

## Section 3: Independent auditor's ISAE 3000 assurance report with limited assurance on information security and measures pursuant to data processing agreements with customers who has used Autoflows as per 11 February 2022

To: ag analytics a/s and ag analytics a/s' customers as data controllers

### Scope

We were engaged to provide assurance about a) ag analytics a/s' description, Section 1, of the supply of Autoflows in accordance with the data processing agreement with costumers as data controllers per 11 February 2022 and about b) the design and implementation of controls related to the control objectives stated in the Description.

ag analytics a/s uses the following sub-suppliers and sub-processors: Host Europe, Alchemer, MailChimp, ScanNet, IT Arkitekterne, Olinecity.io, TMPO and Google Cloud. This statement does not include control objectives and related controls at ag analytics a/s' sub-suppliers and sub-processors.

We express limited assurance in our conclusion.

### ag analytics a/s' responsibilities

ag analytics a/s is responsible for: preparing the Description and the accompanying statement, Section 2, including the completeness, accuracy, and the method of presentation of the Description and statement, providing the services covered by the Description; stating the control objectives; and designing and implementing controls to achieve the stated control objectives.

### Our independence and quality control

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior and ethical requirements applicable to Denmark.

REVI-IT A/S is subject to the International Standard on Quality Control (ISQC 1) and accordingly uses and maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

### Auditor's responsibilities

Our responsibility is to express an opinion on ag analytics a/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 working efficiently.

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 the data processor's description of Autoflows, and about 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 appropriately designed. Our procedures included testing the implementation of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the Description, the appropriateness of the objectives stated therein, and the appropriateness of the criteria specified by the data processor and described in Section 1.

The scope of the actions we have performed, is less than that of an audit report with reasonable assurance. Consequently, the degree of assurance in our conclusion, is significantly lower than the assurance that would have been obtained, if the assurance report had been performed with reasonable assurance.

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

### **Limitations of controls at a data processor**

ag analytics a/s' description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of Autoflows, 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.

## Opinion

Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the *Management's statement*. During the audit work, we have not found any material aspects, which would lead us to form the opinion:

- (a) that the description does not fairly present the supply of Autoflows, as designed, and implemented as of 11. February 2022, and
- (b) that the controls related to the control objectives stated in the Description, not in all aspects were appropriately designed as of 11 February 2022.

## Description of test of controls

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

## Intended users and purpose

This report and the description of tests of controls in Section 4 are intended only for data controllers who have used ag analytics a/s' Autoflows, and 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 Regulation have been complied with.

Copenhagen, 21 February 2022

### REVI-IT A/S

State authorised public accounting firm

Basel Rimon Obari  
Partner, CISA, CISM

Michael Marseen  
State authorised public accountant

## Section 4: Control objectives, controls, tests, and results hereof

We conducted our engagement in accordance with ISAE 3000, assurance engagements other than audits or review of historical financial information.

Our test of the implementation has included the control objectives and attached controls, selected by management and which are stated in the control objectives A-I below. Our test has included the controls, we find necessary to establish reasonable assurance for compliance with the articles stated per 11 February 2022.

Our statement, does not apply to control objectives and attached controls, performed at ag analytics a/s' sub-suppliers and sub-processors.

Further, controls performed at the data controller are not included in this statement.

We performed our test of controls at ag analytics a/s by the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at ag analytics a/s. The interviews have included questions about, how controls are performed.
Observation	Observing how controls are performed.
Inspection	Reading of documents and reports, including description of the performance of the control. This includes reading and assessment of reports and documents to evaluate whether the specific controls are designed in such a way, that they can be expected to be effective when implemented.
Re-performance	Re-performance of controls to verify that the control is working as assumed.

## List of control objectives compared to GDPR-articles, ISO 27701, and ISO 27001/2

Below, control objectives are mapped against the articles in GDPR, ISO 27701 and ISO 27001/2.

Articles and points about main areas are written in bold.

Control activity	GDPR articles	ISO 27701	ISO 27001/2
<b>A.1</b>	5, 26, <b>28</b> , 29, 30, 32, 40, 41, 42, 48	8.5.5, 5.2.1, 6.12.1.2, 6.15.1.1, 8.2.1, <b>8.2.2</b>	<i>New scope compared to ISO 27001/2</i>
<b>A.2</b>	<b>28</b> , 29, 48	8.5.5, 6.15.2.2, <b>6.15.2.2</b>	18.2.2
<b>A.3</b>	<b>28</b>	<b>8.2.4, 6.15.2.2</b>	18.2.2
<b>B.1</b>	31, <b>32</b> , 35, 36	<b>5.2.2</b>	4.2
<b>B.2</b>	<b>32</b> , 35, 36	<b>7.2.5, 5.4.1.2, 5.6.2</b>	6.1.2, 5.1, 8.2
<b>B.3</b>	<b>32</b>	<b>6.9.2.1</b>	<b>12.2.1</b>
<b>B.4</b>	28 stk. 3; litra e, <b>32</b> ; <b>stk. 1</b>	<b>6.10.1.1, 6.10.1.2, 6.10.1.3, 6.11.1.3</b>	<b>13.1.2, 13.1.3, 14.1.3, 14.2.1</b>
<b>B.5</b>	32	6.6.1.2, 6.10.1.3	9.1.2, 13.1.3, 14.2.1
<b>B.6</b>	<b>32</b>	<b>6.6</b>	9.1.1, 9.2.5
<b>B.7</b>	<b>32</b>	<b>6.9.4</b>	12.4
<b>B.8</b>	<b>32</b>	<b>6.15.1.5</b>	18.1.5
<b>B.9</b>	<b>32</b>	<b>6.9.4</b>	12.4
<b>B.10</b>	<b>32</b>	<b>6.11.3</b>	14.3.1
<b>B.11</b>	<b>32</b>	<b>6.9.6.1</b>	12.6.1
<b>B.12</b>	28, <b>32</b>	<b>6.9.1.2, 8.4</b>	12.1.2
<b>B.13</b>	<b>32</b>	<b>6.6</b>	9.1.1
<b>B.14</b>	<b>32</b>	<b>7.4.9</b>	<i>New scope compared to ISO 27001/2</i>
<b>B.15</b>	<b>32</b>	<b>6.8</b>	11.1.1-6
<b>C.1</b>	<b>24</b>	<b>6.2</b>	5.1.1, 5.1.2
<b>C.2</b>	<b>32, 39</b>	<b>6.4.2.2, 6.15.2.1, 6.15.2.2</b>	7.2.2, 18.2.1, 18.2.2
<b>C.3</b>	<b>39</b>	<b>6.4.1.1-2</b>	7.1.1-2
<b>C.4</b>	28, 30, <b>32, 39</b>	<b>6.10.2.3, 6.15.1.1, 6.4.1.2</b>	7.1.2, 13.2.3
<b>C.5</b>	<b>32</b>	<b>6.4.3.1, 6.8.2.5, 6.6.2.1</b>	7.3.1, 11.2.5, 8.3.1
<b>C.6</b>	<b>28, 38</b>	<b>6.4.3.1, 6.10.2.4</b>	7.3.1, 13.2.4
<b>C.7</b>	<b>32</b>	<b>5.5.3, 6.4.2.2</b>	7.2.2, 7.3
<b>C.8</b>	<b>38</b>	<b>6.3.1.1, 7.3.2</b>	6.1.1
<b>C.9</b>	6, 8, 9, 10, 15, 17, 18, 21, 28, <b>30, 32</b> , 44, 45, 46, 47, 48, 49	6.12.1.2, 6.15.1.1, 7.2.2, <b>7.2.8</b> , 7.5.1, 7.5.2, 7.5.3, 7.5.4, <b>8.2.6</b> , 8.4.2, 8.5.2, 8.5.6	<i>New scope compared to . ISO 27001/2</i>
<b>D.1</b>	6, 11, <b>13, 14, 32</b>	<b>7.4.5, 7.4.7, 7.4.4</b>	<i>New scope compared to . ISO 27001/2</i>
<b>D.2</b>	6, 11, 13, 14, <b>32</b>	<b>7.4.5, 7.4.7, 7.4.4</b>	<i>New scope compared to . ISO 27001/2</i>
<b>D.3</b>	13, <b>14</b>	<b>7.4.7, 7.4.4</b>	<i>New scope compared to . ISO 27001/2</i>
<b>E.1</b>	13, 14, <b>28, 30</b>	<b>8.4.2, 7.4.7, 7.4.8</b>	<i>New scope compared to . ISO 27001/2</i>
<b>E.2</b>	13, 14, <b>28, 30</b>	<b>8.4.2, 7.4.7, 7.4.8</b>	<i>New scope compared to . ISO 27001/2</i>
<b>F.1</b>	6, 8, 9, 10, 17, 18, 22, 24, 25, 28, <b>32</b> , 35, 40, 41, 42	5.2.1, <b>7.2.2, 7.2.6</b> , 8.2.1, 8.2.4, 8.2.5, 8.4.2, 8.5.6, 8.5.7	15
<b>F.2</b>	<b>28</b>	<b>8.5.7</b>	15
<b>F.3</b>	<b>28</b>	<b>8.5.8, 8.5.7</b>	15

<b>F.4</b>	<b>33, 34</b>	<b>6.12.1.2</b>	15
<b>F.5</b>	<b>28</b>	<b>8.5.7</b>	15
<b>F.6</b>	<b>33, 34</b>	<b>6.12.2</b>	15.2.1-2
<b>G.1</b>	15, 30, <b>44, 45</b> , 46, 47, 48, 49	<b>6.10.2.1, 7.5.1</b> , 7.5.2, 7.5.3, 7.5.4, <b>8.5.1</b> , 8.5.2, 8.5.3	13.2.1, 13.2.2
<b>G.2</b>	15, 30, <b>44, 45</b> , 46, 47, 48, 49	<b>6.10.2.1, 7.5.1</b> , 7.5.2, 7.5.3, 7.5.4, <b>8.4.2</b> , 8.5.2, 8.5.3	13.2.1
<b>G.3</b>	15, 30, <b>44, 45</b> , 46, 47, 48, 49	<b>6.10.2.1, 7.5.1</b> , 7.5.2, 7.5.3, 7.5.4, 8.5.3	13.2.1
<b>H.1</b>	12, <b>13, 14</b> , 15, 20, 21	<b>7.3.5, 7.3.8, 7.3.9</b>	<i>New scope compared to . ISO 27001/2</i>
<b>H.2</b>	12, <b>13, 14</b> , 15, 20, 21	<b>7.3.5, 7.3.8, 7.3.9</b>	<i>New scope compared to . ISO 27001/2</i>
<b>I.1</b>	<b>33, 34</b>	<b>6.13.1.1</b>	16.1.1-5
<b>I.2</b>	<b>33, 34</b> , 39	6.4.2.2, <b>6.13.1.5, 6.13.1.6</b>	16.1.5-6
<b>I.3</b>	<b>33, 34</b>	<b>6.13.1.4</b>	16.1.5
<b>I.4</b>	<b>33, 34</b>	<b>6.13.1.4</b> , 6.13.1.6	16.1.7



## Control objective A - Instructions regarding processing of personal data

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

No.	ag analytics a/s' control activity	REVI-IT A/S' performed test	Result of 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>We have inquired into whether formalized procedures exist to ensure that personal data are only processed according to instructions.</p>	<p>We have been informed, that there is no procedure to ensure that instructions are being followed.</p> <p>No further deviations noted.</p>
A.2	<p>The data processor only processes personal data stated in the instructions from the data controller.</p>	<p>We have inquired into how management ensures that personal data are only processed according to instructions, and we have assessed whether the instructions are suitable.</p> <p>We have inspected documentation that instructions are being received for the processing.</p>	<p>No deviations noted.</p>
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>We have inspected that formalised procedures exist, ensuring verification that personal data are not processed against the Regulation or other legislation.</p> <p>We have assessed whether it is likely that the data controller will be informed if instructions according to the data processor is evaluated to be in violation of general data protection regulation or data protection regulations in other EU-law or Member States' national law.</p>	<p>We have been informed, that there is no procedure for the information of the data controller, if and instruction is in violation of the general data protection regulation or data protection regulations in other EU-law or Member States' national law.</p> <p>No further deviations noted.</p>

## Control objective B - Technical measures

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

No.	ag analytics a/s' control activity	REVI-IT A/S' performed test	Result of 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>We have inquired, whether formalized procedures are available, to ensure that the agreed security measures are established.</p>	<p>We have been informed, that there is no procedure requiring that the agreed security measures are established.</p> <p>No further deviations noted.</p>
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>We have inquired into whether formalized procedures are established, to ensure that data processor is performing a risk assessment, to achieve an adequate level of security.</p> <p>We have inquired with data processor, which technical measures have been implemented and how these ensures an adequate level of security according to the risk assessment.</p> <p>We have inspected documentation, that data processor has implemented the security measures, agreed with one single selected data controller.</p>	<p>No deviations noted.</p>
B.3	<p>For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.</p>	<p>We have inspected that, for the systems and databases used in the processing of personal data, antivirus software has been installed.</p> <p>We have inspected that antivirus software is installed and updated on a system.</p>	<p>No deviations noted.</p>
B.4	<p>External access to systems and databases used in the processing of personal data takes place through a secured firewall.</p>	<p>We have inspected that external access to systems and databases used in the processing of personal data takes place only through a secured firewall.</p> <p>We have inspected documentation that the firewall is active.</p>	<p>No deviations noted.</p>

## Control objective B - Technical measures

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

No.	ag analytics a/s' control activity	REVI-IT A/S' performed test	Result of test
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	<p>We have inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.</p> <p>We have inspected network diagrams and other network documentation, to assess whether segmentation is appropriate.</p>	No deviations noted.
B.6	Access to personal data is isolated to users with a work-related need for such access.	<p>We have inquired into whether formalized procedures are established to limit users' access to personal data.</p> <p>We have inquired whether formalized procedures are established, for periodically review of whether users' access to personal data are according to their work-related needs.</p> <p>We have inspected documentation, that periodic review has been performed, according to the plan.</p> <p>We have inspected, that users' access to systems and databases, are limited to their work-related needs.</p>	No deviations noted.
B.7	For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature.	<p>We have inspected that, for systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature.</p> <p>We have – by sample test of one alarm – inspected that the alarm was followed up on.</p>	No deviations noted.

## Control objective B - Technical measures

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

<i>No.</i>	<i>ag analytics a/s' control activity</i>	<i>REVI-IT A/S' performed test</i>	<i>Result of test</i>
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	<p>We have inspected 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>We have inquired whether technological solutions for encryption have been available and activated during the period.</p> <p>We have – by a few sample tests – inspected whether setup of transmission paths is efficiently encrypted.</p> <p>We have inquired whether any unencrypted transmission of sensitive and confidential personal data has taken place and whether the data controllers have been appropriately informed thereof.</p>	No deviations noted.

## Control objective B - Technical measures

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

No.	ag analytics a/s' control activity	REVI-IT A/S' performed test	Result of test
B.9	<p>Logging has been established in systems, databases, and networks.</p> <p>Logon data are protected against manipulation and technical errors and are reviewed regularly.</p>	<p>We have inspected 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>We have inspected 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>We have inspected that user activity data collected in logs are protected against manipulation and deletion.</p> <p>We have, based on a randomly chosen day's log file inspected, that the log file is as expected compared to the setup, and we have inspected documentation of the follow-up and management of possible security incidents and activities performed by system administrators and others holding special rights etcetera.</p>	No deviations noted.
B.10	<p>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>	<p>We have inspected 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 form.</p>	<p>We have been informed that production data are being used for testing. This data is protected like production data, and it has been ensured that access to the data is based on a work-related need.</p> <p>No further deviations noted.</p>

## Control objective B - Technical measures

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

No.	ag analytics a/s' control activity	REVI-IT A/S' performed test	Result of test
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	<p>We have inspected that formalised procedures exist for regularly testing technical measures, including for performing vulnerability scans and penetration tests.</p> <p>We have inspected documentation of the latest tests of the established technical measures.</p> <p>We have inquired whether possible deviations or weaknesses in the technical measures have been responded to in a timely and appropriately manner and communicated to the data controllers as appropriate.</p>	No deviations noted.
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>We have inspected that formalised procedures exist for handling changes to systems, databases, and networks, including handling of relevant updates, patches, and security patches.</p> <p>We have – by sample test – inspected that relevant patches and security patches are being handled.</p>	No deviations noted.
B.13	A formalised procedure is in place for granting and removing users' access to personal data. Users' access is re-considered on a regular basis, including the continued justification of rights by a work-related need.	<p>We have inquired whether formalized procedures exist for granting and revoking users' access to systems and databases, used for the processing of personal data.</p> <p>We have inspected, that access to systems and databases are based on a work-related need.</p> <p>We have – by a single sample test – inspected whether access to systems and databases have been revoked for a terminated employee.</p> <p>We have inspected documentation, that periodical assessment and approval of granted user accesses has been performed according to the plan.</p>	No deviations noted.

## Control objective C - Organisational measures

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

No.	ag analytics a/s' control activity	REVI-IT A/S' performed test	Result of 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>We have inspected whether an information security policy exists that Management has considered and approved within the past year.</p> <p>We have inquired whether information security policy has been communicated to relevant stakeholders, including data processor's employees.</p>	No deviations noted.
C.2	Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.	We have, for a typical data processing agreement, inspected whether the requirements in the agreements are covered by the requirements of the information security policy for safeguards and security of processing.	No deviations noted.
C.3	The employees of the data processor are screened as part of the employment process.	<p>We have inquired whether formalised procedures are in place to ensure screening of the data processor's employees as part of the employment process.</p> <p>We have – by sample test of a new employee – inquired into whether screening has been performed.</p>	No deviations noted.



## Control objective C - Organisational measures

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

No.	ag analytics a/s' control activity	REVI-IT A/S' performed test	Result of 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>We have inspected that a typical contract of employment includes a confidentiality clause.</p> <p>We have inquired into the procedure for, how the employee is introduced to:</p> <ul style="list-style-type: none"> <li>• Information security policy</li> <li>• Procedures regarding data processing, and other relevant information</li> </ul>	No deviations 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>We have inquired whether procedures exist, 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>We have, by sample test of a terminated employee during the period inspected, that rights have been deactivated or terminated, and that assets have been returned.</p>	No deviations 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>We have inspected 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>We have, by sample test of a terminated employee during the period inspected, that documentation exists for the continued validity of confidentiality agreement and general duty of confidentiality</p>	No deviations noted.

## Control objective C - Organisational measures

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

No.	ag analytics a/s' control activity	REVI-IT A/S' performed test	Result of test
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.	<p>We have inquired whether the data processor provides awareness training to the employees covering general IT security and security of processing related to personal data.</p> <p>We have inquired into how it is ensured, that all employees who have either access to, or process personal data, have completed the awareness training provided.</p>	No deviations noted.
C.8	The processor has assessed the need for a DPO and has ensured that the DPO has the adequate professional competence to perform their tasks and are involved in relevant areas.	We have inquired whether an assessment of the need of a data protection officer is available.	No deviations noted.
C.9	<p>The processor keeps a record of categories of processing activities for each data controller.</p> <p>Management has ensured, that the list of categories of control objectives for each controller include:</p> <ul style="list-style-type: none"> <li>• Name and contact information of the data processor, the data controller's representatives, and data protection officers</li> <li>• The types of processing, performed on behalf of each data controller</li> <li>• When relevant, information about transfer to a third country or an international organisation and also documentation of appropriate guarantees</li> <li>• If possible, a general description of technical and organisational security measures</li> </ul> <p>Regularly – and at least annually – an assessment is made of whether the list should be updated.</p>	We have inspected, that records are present, which management has considered and approved within the last year.	No deviations noted.

## Control objective D - Return and deletion of personal data

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.	ag analytics a/s' control activity	REVI-IT A/S' performed test	Result of 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>We have inquired whether formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller</p> <p>We have inquired into when procedures are being updated, and which updates, if any, have been performed.</p> <p>We have inspected a list of written procedures and assessed, whether this appears to be updated and adequate compared to the agreed storage and deletion of personal data.</p>	No deviations noted.
D.2	<p>Specific requirements have been agreed with respect to the data processor's storage periods and deletion routines.</p>	<p>We have inspected that the existing procedures for storage and deletion include specific requirements for the data processor's storage periods and deletion routines.</p> <p>We have – by sample test – from the data processors list of processing activities inspected, that documentation exists that personal data are being stored according to the agreed storage periods and deletion routines.</p>	No deviations 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>	<p>We have inquired whether formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data.</p> <p>We have, by sample test, inspected that documentation exists that the agreed deletion or return of data has taken place for terminated data processing sessions.</p>	No deviations noted.

## Control objective E – Storage of personal data

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.	ag analytics a/s' control activity	REVI-IT A/S' performed test	Result of 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>We have inquired whether formalised procedures exist for only storing and processing personal data in accordance with the data processing agreements.</p> <p>We have inquired whether the procedures are updated, and if any, which updates have been performed.</p>	No deviations 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>We have inquired whether the data processor has a complete and updated list of processing activities stating localities, countries, or regions.</p> <p>We have inquired whether data processing and storage of data only take place in the approved localities, countries, and regions.</p>	No deviations noted.

## Control objective F – Use of sub-processors

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.

No.	ag analytics a/s' control activity	REVI-IT A/S' performed test	Result of test
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>We have inquired whether formalized procedures exist for the use of sub-data processors including requirements for sub-data processing agreements and instructions.</p> <p>We have inquired, when procedures have been updated and, if any, which updates have been performed.</p> <p>We have inspected the list of written procedures and assessed whether this appears to be updated and adequate compared to the use of sub-data processors.</p>	No deviations noted.
F.2	The data processor only uses sub-data processors to process personal data that have been specifically or generally approved by the data controller.	<p>We have inquired whether the data processor has an overall and updated list of used sub-data processors.</p> <p>We have, by sample test of a single sub-data processor from the data processor's list of sub-data processors inspected, 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. (Specifically, or indirectly)</p>	No deviations noted.
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.	We have inquired whether formalised procedures are in place for informing the data controller when changing the sub-data processors used.	<p>We have been informed, that there have been no changes in the use of sub-data processors during the period, hence we have not tested the implementation of data processor's procedures.</p> <p>No deviations noted.</p>
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.	We have inquired about the existence of signed sub-data processing agreements with sub-data processors used, which are stated on the data processor's list.	No deviations noted.

## Control objective F – Use of sub-processors

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.

No.	ag analytics a/s' control activity	REVI-IT A/S' performed test	Result of test
		<p>We have, by sample test, inspected that sub-data processing agreements include the same requirements and obligations as are stipulated in the data processing agreements between the data controllers and the data processor.</p>	
F.5	<p>The data processor has a list of approved sub-data processors.</p>	<p>We have inquired whether the data processor has a complete and updated list of sub-data processors used and approved.</p> <p>We have – for a single sub-data processor – inspected that the list includes the required information.</p>	<p>No deviations noted.</p>
F.6	<p>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 processor.</p>	<p>We have inquired whether 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>We have inspected documentation that risk assessment has been made of a randomly chosen sub-data processor and the actual processing activity with this processor, and also that follow-up has been planned according to the risk assessment.</p>	<p>No deviations noted.</p>

## Control objective G – Transfer of personal data to third countries

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.	ag analytics a/s' control activity	REVI-IT A/S' performed test	Result of 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>We have inquired whether 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>We have inquired whether procedures are updated and if any, which updates have been made.</p> <p>We have inspected the list of written procedures and assessed whether this appears updated and adequate with regards to transfer of personal data.</p>	No deviations 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>We have inquired whether the data processor has an overall and updated list of transfers of personal data to third countries or international organisations.</p> <p>We have, for a randomly chosen data processing agreement inspected, that it includes instruction about transfer of personal data to third countries.</p>	No deviations noted.
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>We have inquired whether formalised procedures are in place for ensuring a valid basis of transfer.</p> <p>We have inquired when procedures have been updated and if any, which updates have been made.</p> <p>We have inquired whether a valid basis of transfer is included in the data processing agreement with the data controller, and also that transfers only have been performed according to agreement with data controller.</p>	No deviations noted.



## Control objective H – Rights of the data subjects

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.	ag analytics a/s' control activity	REVI-IT A/S' performed test	Result of 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>We have inquired whether 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>We have inquired when procedures have been updated and if any, which updates have been made.</p> <p>We have inspected the list over written procedures and assessed whether this appears to be updated and adequate regarding assistance to the data controller.</p>	No deviations noted.
H.2	<p>The data processor has established procedures as 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>We have inquired whether 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>We have assessed whether it is likely that the systems and databases used, support the performance of the relevant detailed procedures.</p>	No deviations noted.

## Control objective I – Managing personal data breaches

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.	ag analytics a/s' control activity	REVI-IT A/S' performed test	Result of 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>We have inquired whether formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches.</p> <p>We have inquired when procedures have been updated and if any, which updates have been made.</p> <p>We have inspected the list of written procedures and assessed whether this appears to be updated and adequate compared to managing personal data breaches.</p>	No deviations noted.
I.2	<p>The data processor has established the following controls to identify any personal data breaches:</p> <ul style="list-style-type: none"> <li>• Awareness of employees</li> </ul>	We have inquired whether the data processor provides awareness training to the employees in identifying any personal data breaches.	No deviations noted.
I.3	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>We have inquired whether the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach.</p> <p>We have inquired whether the data processor has included any personal data breaches at sub-data processors in the data processor's list of security incidents.</p> <p>We have inquired whether 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>	<p>We have been informed, that there have not been any personal data breaches during the period, wherefore we have not tested the implementation of the data processor's procedures.</p> <p>No deviations noted.</p>

## Control objective I – Managing personal data breaches

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.	ag analytics a/s' control activity	REVI-IT A/S' performed test	Result of test
I.4	<p>The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency:</p> <ul style="list-style-type: none"> <li>• Nature of the personal data breach</li> <li>• 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>We have inquired whether the procedures established for informing the data controllers in the event of any personal data breach include detailed procedures for:</p> <ul style="list-style-type: none"> <li>• Describing the nature of the personal data breach</li> <li>• Describing the probable consequences of the personal data breach</li> <li>• Describing measures taken or proposed to be taken to respond to the personal data breach.</li> </ul> <p>We have assessed whether it is likely that the established procedures support, that measures are taken to respond to the personal data breach.</p>	No deviations noted.