

# Self-assessment report

---

Second level of organization test  
address  
900 test  
test  
Company registration number: 00000000  
(the "**Company**")

This is version 1, last updated the 04.03.2021 10:12.

## 1. Introduction

- 1.1 This document is a report (the "**Report**") prepared to document the Company's ongoing efforts and measures to comply with the applicable data protection and privacy legislation, including in particular the EU General Data Protection Regulation (2016/679 of 27 April 2016) (the "**GDPR**") and the requirement of demonstrating compliance (the principle of "accountability") as described in article 5(2) of the GDPR.
- 1.2 The report shall apply to the entire Company and all of its systems and business processes.
- 1.3 The Report contains color markings with green, yellow and red markings at the Company's results of the control objectives. The colors do not necessarily mean that the Company complies with the GDPR, but they help to identify any areas and issues that the Company should work with as described.
- 1.4 The Report and the Company's comments and controls cover the period since the latest prepared Report and until the date of this Report. Each Report shall cover the foregoing period.

## 2. Control method and structure

- 2.1 The Report is prepared on the basis of the Company's answers on questions and control points in ComplyCloud.
- 2.2 When and if the Danish Data Protection Agency publishes guidance on self assessment these guidelines will be incorporated in the questions and control points in the Report.

## 3. General information about the controls

- 3.1 The Company follows a systematic approach for documenting GDPR compliance and uses an annual cycle of work to ensure automatic and continuous controls with reminders. This means, among other things, that the Company reviews and updates all procedures, policies, records of processing activities and instructions continuously to ensure that they are updated and correct. The management is also included in the assessment and approval of these reports. Controls concerning auditing, updating and management review and approval are therefore not further commented below as reference is made to the underlying documentation for documenting these control points as appropriate.

## 4. Principles relating to processing of personal data (article 5)

### 4.1 Control objective


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

## 4.2 Control 1

Control activity: Written procedures are available in which the following principles relating to processing of personal data have been considered: (i) lawfulness, fairness and transparency; (ii) purpose limitation; (iii) data minimisation; (iv) accuracy; (v) storage limitation; (vi) integrity and confidentiality; and (vii) accountability.

Performed control: Inspected that there are updated written procedures for processing of personal data that include the principles relating to processing of personal data.

Result of control:

 It cannot be confirmed for certain that the Company has employee instructions, procedures or policies that inform the Company's employees about the principles relating to processing of personal data as set out in article 5 of the GDPR. The Company will as soon as possible as part of its continuous work to ensure compliance with the GDPR make sure that such instructions, procedures and/or policies are procured or prepared and distributed to the employees who work with and process personal data. Alternatively, the Company will update the necessary existing instructions, procedures and/or policies and distribute the new version to such employees.

## 5. Lawfulness of processing (article 6)

### 5.1 Control objective


Procedures and controls are complied with to ensure that personal data is only processed lawfully.

### 5.2 Control 1

Control activity: There is continuously performed assessments of whether illegal processing of personal data has taken place, and these assessments are documented.

Performed control: Inspected documentation for continuous — and at least annually — assessment of whether illegal processing of personal data has taken place.

Result of control:

 The Company is not aware of any unlawful processing of personal data.

### 5.3 Control 2

Control activity: Written procedures are available in which it has been specified that processing of personal data is only allowed when there is a legal basis. There is an ongoing - and at least once a year - assessment of whether the procedures need to be updated and whether the procedures are complied with.

Performed control: Inspected that the Company has updated written procedures for the processing of personal data specifying that personal data processing is only allowed when there is a legal basis.

Result of control:

- ✅ The Company has employee instructions that apply to the Company's employees who work with and process personal data. In these the Company has obliged its employees to only process personal data when there is a legal basis for the processing, including a legal basis that is in accordance with any applicable instructions from data processing agreements with data controllers. Furthermore, the Company continuously—and at least annually—review the employee instructions to assess whether updates are necessary and whether the employee instructions has been complied with by the Company's employees.

#### 5.4 **Kontrol 3**

Control activity: The written procedures in control 2 are available for Company employees.

Performed control: Inspected that the procedures are available for the employees.

Result of control:

- ❗ **GAP:** The Company cannot confirm that the procedures are available for the employees. This is necessary, however, to achieve compliance with the procedures. In other words, employees cannot follow procedures that they do not know, and it is therefore necessary for the employees to have access to the procedures. The Company will therefore as soon as possible make the procedures available for the relevant persons and communicate them as appropriate in order to comply with the GDPR.

### 6. **Consent (article 7 and 8)**

#### 6.1 **Control objective**

Procedures and controls are complied with to ensure that the data subjects provide written consent for the processing of personal data when necessary.

#### 6.2 **Control 1**

Control activity: There are written procedures for collecting written consent for the processing of personal data. There is an ongoing - and at least once a year - assessment of whether the procedures need to be updated and whether the procedures are complied with.

Performed control: Inspected that there are written procedures for obtaining written consent for processing personal data.

Result of control:

## 7. **Processing special categories of personal data (article 9 and 10)**

### 7.1 **Control objective**

Procedures and controls are complied with to ensure that special categories of personal data are only processed when specified criteria, conditions and necessary guarantees have been considered.

### 7.2 **Control 1**

Control activity: There is an instruction that is approved which regulates the Company's processing of special categories of personal data.

Performed control: Inspected that it is documented that the processing of special categories of personal data is done on a legal processing basis.

Result of control:

- ❌ The Company does not process special categories as part of the processing of personal data.

## 8. **Processing which does not require identification (article 11)**

### 8.1 **Control objective**

Procedures and controls are complied with to ensure that storage, collection and processing of information for identifying the data subject is maintained as long as identification is required.

### 8.2 **Control 1**

Control activity: There are procedures and controls to ensure that storage, collection and processing of information for identifying the data subject is maintained as long as identification is required. Assessments are continuously made - and at least once every year - about whether the procedures should be updated.

Performed control: Inspected that there are updated written procedures to ensure that it has been considered that storage, collection and processing of information for the identification of the data subject is maintained as long as identification is required.

Result of control:

The Company does not process personal data in such a way that article 11 of the GDPR is relevant.

## 9. **Transparent information, communication and modalities for the exercise of the rights of the data subject (article 12)**

### 9.1 **Control objective**


Procedures and controls are complied with to ensure that information about the processing of personal data can be provided and communicated in a concise, transparent, intelligible and easily accessible form to the data subject.

### 9.2 **Control 2**

Control activity: It is continuously ensured - and at least once every year - that replies to requests from data subjects are completed in due time.

Performed control: Inspected documentation for that actual replies of the requests from data subjects have been performed in due time and in accordance with procedures.

Result of control:

-  The Company has not implemented processes and procedures to ensure that the Company continuously and at least once every year answers all inquiries and requests from data subjects correctly and in a timely manner. The Company will make such controls as soon as possible as part of its continuous work to comply with the GDPR.

## 10. **Information to be provided where personal data are collected (article 13 and 14)**

### 10.1 **Control objective**

Procedures and controls are complied with to ensure that the data subject has received the Company's contact information, information about the purpose(s) of the processing of personal data in addition to information about any transfer of personal data to recipients in third countries or international organisations.

### 10.2 **Control 1**

Control activity: There are written procedures describing how it is ensured that the data subject receives information about the purpose(s) of the processing of personal data in addition to information about any transfer of personal data to recipients, third countries or international organisations, or how the data processor can assist the data controller in this manner. Assessments are continuously made - and at least once every year - about whether the procedures should be updated.

Performed control: Inspected that there are updated written procedures in which it is

described how it is ensured that the data subjects receives information about the purpose(s) about the processing of personal data in addition to information about any transfer of personal data to recipients, third countries or international organisations.

Result of control:

- ❗ The personal data policies of the Company do not contain the necessary information for the data subjects, which is required under article 13 and 14 of the GDPR. The Company will prepare such a policy as soon as possible as a part of its continuous work to comply with the GDPR.

## 11. **The data subject's right of access (article 15)**

### 11.1 **Control objective**

Procedures and controls are complied with to ensure the data subject's right of access in own personal data.

### 11.2 **Control 1**

Control activity: The Company has a defined format for extracting personal data (copy of the personal data which are registered and processed by the Company) to the data subject.

Performed control: Inspected that the Company has a defined format for extracting personal data to the data subject.

Result of control:

- ⚠ The Company has not defined formats and methods to use when delivering copies of personal data in accordance with article 15(2) of the GDPR. The Company will define such formats and methods/processes as soon as possible as part of its continuous efforts to comply with the GDPR.

### 11.3 **Control 2**

Control activity: Written procedures exist in which the handling of the data subject's requests about access in the processing of personal data is described. Assessments are continuously made - and at least once every year - about whether the procedures should be updated.

Performed control: Inspected that there are updated written procedures in which the handling of the data subjects requests for access in his/her personal data are described.

Result of control:

- ! The Company does not have procedures on how to comply with the data subject's right of access in accordance with article 15 of the GDPR. The Company will prepare such procedures as soon as possible as a part of its continuous work to comply with the GDPR.

## 12. **Right to rectification (article 16 and article 19)**

### 12.1 **Control objective**

Procedures and controls are complied with to ensure that the data subjects' right to rectification of personal data about him/her, including rectification at the recipients' of the personal data, are complied with.

### 12.2 **Control 1**

Control activity: Technical measures have been established in the Company's IT systems which ensures that personal data can be corrected.

Performed control: Inspected that technical measures have been established in the Company's IT systems in order to correct personal data. Inspected that the rectification of personal data only takes place through the established technical measures.

Result of control:

- ! It cannot be confirmed with certainty that the IT-systems of the Company supports the rectification of personal data. The Company will as soon as possible as part of its continuous work to comply with the GDPR continue its work on the IT-systems and plan how to ensure this going forward.

### 12.3 **Control 2**

Control activity: The Company has written procedures after which the handling of the data subjects' right to rectification of personal data is described. There is an ongoing - and at least once a year - assessment of whether the procedures need to be updated and whether the procedures are complied with.

Performed control: Inspected that there are updated written procedures for handling the data subjects' rights to rectification of personal data.

Result of control:

- ! The Company does not have procedures on how to comply with the data subject's right to rectification in accordance with article 16 of the GDPR.



### 13. **Right to erasure (article 17 and article 19)**

#### 13.1 **Control objective**

Procedures and controls are complied with in order to ensure that the data subjects' right to erasure of personal data about him/her are complied with, including erasure of personal data at the recipients of the personal data.

#### 13.2 **Control 1**

Control activity: Technical measures have been implemented in the Company's IT system to ensure that it is possible to erase personal data.

Performed control: Inspected that technical measures have been established in the Company's IT system in order to erase personal data. Inspected that personal data are only erased by using the established technical measures.

Result of control:

- ❗ It cannot be confirmed with certainty that the IT-systems of the Company supports the erasure of personal data in accordance with article 17 of the GDPR. The Company will as soon as possible as part of its continuous work to comply with the GDPR continue its work on the IT-systems and plan how to ensure this going forward.

#### 13.3 **Control 2**

Control activity: The Company has written procedures in which the handling of the data subjects' right to erasure of personal data are described. There is an ongoing - and at least once a year - assessment of whether the procedures need to be updated and whether the procedures are complied with.

Performed control: Inspected that the Company has written and updated procedures for the handling of the data subject's right to erasure of personal data.

Result of control:

- ❗ The Company does not have procedures on how to comply with the data subject's right to erasure in accordance with article 17 of the GDPR. The Company will prepare such procedures as soon as possible as a part of its continuous work to comply with the GDPR.

### 14. **Right to restriction of processing (article 18 and article 19)**

#### 14.1 **Control objective**

Procedures and controls are complied with in order to ensure that the data subject's right to restriction of processing, including restriction at the recipients of the personal

data, is complied with.

#### 14.2 **Control 1**

Control activity: There has been implemented technical measures in the IT systems to ensure that it is possible to restrict a processing of personal data.

Performed control: Inspected that technical measures has been implemented in the Company's IT-system in order to restrict a processing of personal data. Inspected that a restriction of a processing of personal data only happens by the use of the implemented technical measures.

Result of control:

- ❗ It cannot be confirmed with certainty that the IT-systems of the Company supports the restriction of personal data processing in accordance with article 18 of the GDPR. The Company will as soon as possible as part of its continuous work to comply with the GDPR continue its work on the IT-systems and plan how to ensure this going forward.

#### 14.3 **Control 2**

Control activity: The Company has written and updated procedures in which the handling of the data subjects' right to restriction of a processing of their personal data is described. There is an ongoing - and at least once a year - assessment of whether the procedures need to be updated and whether the procedures are complied with.

Performed control: Inspected that there are updated written procedures for the handling of the data subjects' rights to restriction of a processing of personal data.

Result of control:

- ❗ The Company does not have procedures on how to comply with the data subject's right to erasure in accordance with article 18 of the GDPR. The Company will prepare such procedures as soon as possible as a part of its continuous work to comply with the GDPR.

### 15. **Right to data portability (article 20)**

#### 15.1 **Control objective**

Procedures and controls are complied with in order to ensure the data subject's right to transfer personal data about him/her to another data controller.

#### 15.2 **Control 1**

Control activity: Technical measures have been implemented in the Company's IT

system to ensure the data subjects' right to data portability.

Performed control: Inspected that technical measures have been implemented in the Company's IT system to ensure the data subjects' right to data portability.

Result of control:

- ❗ It cannot be confirmed with certainty that the IT-systems of the Company supports the data subject's right to data portability in accordance with article 20 of the GDPR. The Company will as soon as possible as part of its continuous work to comply with the GDPR continue its work on the IT-systems and plan how to ensure this going forward.

### 15.3 Control 2

Control activity: There are written procedures in the data subject's right to transfer personal data about him/her is described. There is an ongoing - and at least once a year - assessment of whether the procedures need to be updated and whether the procedures are complied with.

Performed control: Inspected that there are updated written procedures for the data subject's right to transfer personal data about him/her to another data controller.

Result of control:

- ❗ The Company does not have procedures on how to comply with the data subject's right to data portability in accordance with article 20 of the GDPR. The Company will prepare such procedures as soon as possible as a part of its continuous work to comply with the GDPR.

## 16. Data protection by design and by default (article 25)

### 16.1 Control objective

Procedures and controls are complied with in order to ensure that the requirements for data protection by design and by default in are complied with in the Company's technical measures.

### 16.2 Control 1

Control activity: The Company has written procedures in which data protection by design and by default has been described. There is an ongoing - and at least once a year - assessment of whether the procedures need to be updated and whether the procedures are complied with.

Performed control: Inspected that the Company has updated written procedures for ensuring data protection by design and by default.

Result of control:

- ⚠ The Company does not have procedures that apply to the employees of the Company that work with and process the personal data. The Company therefore does not have documented instruction to be used by its employees to follow to ensure that compliance with article 25 of the GDPR on data protection by design and by default.

## 17. **Records of processing activities (article 30)**

### 17.1 **Control objective**

Procedures and controls are complied with in order to ensure that the Company maintains records of processing activities.

### 17.2 **Control 1**

Control activity: The Company has a record of processing activities.

Performed control: Inspected that the Company has a record of processing activities.

Result of control:

- ❗ It cannot be confirmed for certain that the Company has prepared records of categories of processing activities in accordance with article 30 of the GDPR. The Company will as soon as possible rectify this as part of its continuous work to ensure compliance with the GDPR by preparing such records of processing activities.

## 18. **Security of processing (article 32)**

### 18.1 **Control objective**

Procedures and controls are complied with in order to ensure that the Company has implemented technical and organizational measures based on a risk assessment in order to prevent accidental or illegal destruction, loss, alteration, unauthorized disclosure or access to personal data.

### 18.2 **Control 1**

Control activity: The Company has made an risk assessment of the processing of personal data, including the preparation of the Company's security descriptions.

Performed control: Inspected that the Company has made a risk assessment of a processing of personal data, including the preparation of the Company's security descriptions.

Result of control:

- ❗ The Company has not assessed the specific risk for the data processing in connection with determining the security measures. The Company will as soon as possible as part of its continuous efforts to comply with the GDPR make sure to assess whether the described risk are covered by the implemented security measures.

### 18.3 **Control 2**

Control activity: The Company has implemented appropriate technical and organisational security measures which cover the risk in the Company's risk assessment.

Performed control: Inspected that the Company has implemented appropriate technical and organisational security measures which cover the risk in the Company's risk assessment.

Result of control:

## 19. **Personal data breach (article 33 and article 34)**

### 19.1 **Control objective**

Procedure and controls are complied with in order to ensure that the Company is able to make adequate notification of a personal data breach to the supervisory authority as well as communicating the breach to the persons affected.

### 19.2 **Control 1**

Control activity: The Company ensures that all personal data breaches are registered and documented.

Performed control: Inspected that the Company has registered and documented all personal data breaches.

Result of control:

- ❗ The Company does not continuously and systematically registers any personal data breaches regardless of whether such breaches are to be notified to the supervisory authorities, i.e. the data protection agencies, in accordance with the documentation requirement of article 33(5) of the GDPR. The Company will as soon as possible as part of its continuous work to comply with the GDPR ensure that such registrations occur and include the necessary information, such as information about the facts relating to each personal data breach, its effects and

the remedial actions taken.

### 19.3 **Control 2**

Control activity: Written procedures are available - and updated at least once a year - in which handling of a personal data breach is described.

Performed control: Inspected that written procedures are available in which handling of a personal data breach is described.

Result of control:

- ❗ The Company does not use procedures for handling personal data breaches in accordance with article 33 and 34 of the GDPR. The Company will as soon as possible as part of its continuous efforts to comply with the GDPR prepare or procure such procedures that contain the specifics of how to properly handle personal data breaches, including the notification of personal data breaches to the supervisory authorities and communication to the data subjects.

## 20. **Transfer of personal data(article 44-50)**

### 20.1 **Control objective**

Procedures and controls are complied with in order to ensure that transfer of personal data to a third-country or an international organisation only happens if a legal basis for transfer exists.

### 20.2 **Control 1**

Control activity: To the extent that personal data is transferred to third countries, there is a legal basis for transfer

Performed control: Inspected that there is a legal basis for transfer of personal data to third countries.

Result of control:

- ❗ To the extent that the Company transfers personal data to so-called third countries outside the EU/EEA, the Company has not yet provided documentation of a correct and legal basis for transfer in accordance with GDPR, article 44-50. The Company will as soon as possible as part of its continuous efforts to comply with the GDPR ensure to update this documentation.

## 21. **Contact**

21.1 If you have any questions or comments to the Report, please contact test.

## 22. **Signatures**

22.1 The content and correctness of the Report are hereby confirmed by the Company.



---

mbi

IP-address: 37.57.19.195:27561

Time of signature: 04-03-2021 at: 09:20:43

Signed with esignatur EasySign



This document is signed with esignatur. Embedded in the document is the original agreement document and a signed data object for each signatory. The signed data object contains a mathematical hash value calculated from the original agreement document, which secures that the signatures is related to precisely this document only. Prove for the originality and validity of signatures can always be lifted as legal evidence.

The document is locked for changes and all cryptographic signature certificates are embedded in this PDF. The signatures therefore comply with all public recommendations and laws for digital signatures. With esignatur's solution, it is ensured that all European laws are respected in relation to sensitive information and valid digital signatures. If you would like more information about digital documents signed with esignatur, please visit our website at [www.esignatur.dk](http://www.esignatur.dk).