

## Self-assessment – mSystems ApS

### ISO 27001 · GDPR · Data Processing Agreements

---

#### Resumé

This self-assessment provides an overall insight into the company's work with information security and data protection.

The company is an EU-based SaaS provider operating as a data processor for its customers. An Information Security Management System (ISMS) has been established based on ISO/IEC 27001.

The company processes ordinary personal data as well as CPR numbers on behalf of its customers. The processing is carried out in compliance with the GDPR, and appropriate technical and organisational security measures have been implemented.

Data processing agreements (DPAs) are concluded with customers in accordance with Article 28 of the GDPR, and any sub-processors are engaged in a controlled manner and within the EU.

This statement has been prepared for customers and business partners as documentation of the company's maturity and accountability in the areas of information security and data protection.

---

#### Management statement

The Management hereby declares that the information contained in this self-assessment is accurate and true as of the date of signature

Date: 20-02-2026

Name: Anja Kjeldahl Østergaard

Titel: Director

Signature:



## Annex A – Self-assessment

### Maturity model scale:

0 = Not established

1 = Partially established

2 = Established

3 = Established and documented

---

## ISO 27001 – Informationssikkerhed

### An approved information security policy is in place

0  1  2  3

Comment / explanation:

- mSystems ApS is ISO 27001 compliant

### Roles and responsibilities for information security are defined.

0  1  2  3

Comment / explanation:

### Systematic risk assessments are carried out.

0  1  2  3

Comment / explanation:

- At least once annually or in connection with significant changes to systems or the business.

### Access control is based on the principle of least privilege

0  1  2  3

Comment / explanation:

### A procedure for handling security incidents is in place.

0  1  2  3

Comment / explanation:

- Yes - These are set out in Annex A.16.

**Suppliers and sub-processors are assessed from an information security perspective.**

0  1  2  3

Comment / explanation:

- Yes, all suppliers and sub-processors are carefully assessed before a collaboration is initiated. We receive updates if a supplier's/sub-processor's compliance status or Data Processing Agreement (DPA) changes, and we assess whether such changes mean that the supplier/sub-processor can no longer act as our supplier/sub-processor. In addition, we conduct supervision of them at least once annually.

**GDPR**

**The company's role as a data processor is clearly defined.**

0  1  2  3

Comment / explanation:

**Records of Processing Activities (ROPA) are maintained.**

0  1  2  3

Comment / explanation:

**Technical and organisational measures have been implemented.**

0  1  2  3

Comment / explanation:

**A procedure for handling data subjects' rights is in place.**

0  1  2  3

Comment / explanation:

**Is a register of security incidents maintained, including an indication of whether each individual incident resulted in a personal data breach?**

0  1  2  3

Comment / explanation:

- Yes - This is documented in our incident log, which is kept up to date at all times.

**A procedure for handling personal data breaches is in place.**

0  1  2  3

Comment / explanation:

- Yes - These are set out in Annex A.16.

**Have any personal data breaches been identified in the past 12 months?**

0  1  2  3

Comment / explanation:

- No

**Processing of CPR numbers is carried out in a controlled and documented manner.**

0  1  2  3

Comment / explanation:

- The data controller obtains the customer's consent for the processing of the CPR number. If such consent is not granted, the CPR number is not processed.
- The CPR number is masked when scanning the customer's driving licence, ensuring that the CPR number cannot be viewed afterwards.
- The CPR number is not stored anywhere in the database unless it has been manually entered by an employee, for example in an external note, internal note, or other free-text fields.

## **Data Processing Agreements (DPAs)**

**Data Processing Agreements are concluded with all customers.**

0  1  2  3

Comment / explanation:

- mSystems' current standard Data Processing Agreement (DPA) is available on our website:  
<https://msystems.dk/>

**The Data Processing Agreements comply with Article 28 of the GDPR.**

0  1  2  3

Comment / explanation:

**Sub-processors are identified and documented.**

0  1  2  3

Comment / explanation:

- These are set out in Appendix B of the DPA

**Sub-processors are located within the EU**

0  1  2  3

Comment / explanation:

- Yes

**The security level of sub-processors is monitored**

0  1  2  3

Comment / explanation:

- Yes, all suppliers and sub-processors are carefully assessed before a collaboration is initiated. We receive updates if a supplier's/sub-processor's compliance status or Data Processing Agreement (DPA) changes, and we assess whether such changes mean that the supplier/sub-processor can no longer act as our supplier/sub-processor. In addition, we conduct supervision of them at least once annually.

**Have any sub-processors been replaced within the 12 months?**

0  1  2  3

Comment / explanation:

- Yes, SMTP2GO and Brevo have been added and replace ScanNet's SMTP solution. SMTP2GO and Brevo were subject to due diligence and security assessment prior to implementation. SMTP2GO and Brevo are listed in the current Data Processing Agreement (DPA).
- Criipto has changed its name to Idura.