Microsec zrt.

NIS2, DORA, and Data Act Guide

V1.3

Content

1 Introduction

The European Union has adopted several new regulations and directives governing the IT sector, which stipulate various tests, classifications, or categorizations of products and services, and require monitoring of suppliers/third-party service providers.

These legal regulations are as follows:

- **Data Act** – Regulation (EU) 2023/2854[1] on connected products and services
- **NIS2 Directive** – Directive 2022/2555/EU[2] and its national regulations, which aim to achieve higher IT security
- **DORA Regulation** – Regulation 2022/2554/EU[3] on the resilience of the financial sector (i.e. the banking-specific provisions of NIS2)

Microsec Ltd. has compiled this document for the purpose of facilitating compliance with the above legislation for its customers.

This document contains information on:

- the legislation,
- the classification principles,
- the preliminary classification, and
- where applicable, how to most easily verify compliance with the requirements.

If your organization is subject to any of the above regulations, please refer to the relevant sections.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R2854

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2554

2 The Data Act

Regulation (EU) 2023/2854 of the European Parliament and of the Council on harmonised rules for fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (hereinafter referred to as the Data Act) sets out four main objectives, which are as follows:

1. **Ensuring data access for users**

   The main objective is to give users, whether individuals or businesses, back control over the data they generate.

   - The regulation obliges data controllers (e.g. manufacturers of connected products such as smart devices and industrial machines) to provide users with access to their data.
   - Users can access the data generated by their products free of charge and easily and can transfer it to a third party of their choice (e.g., a repair service or a new service provider).

2. **Encouraging B2B data sharing**

   The regulation also creates a legal framework for businesses (especially SMEs) to access data held by larger players, thereby encouraging innovation and competition.

   - Data holders must share data with third parties on fair, reasonable, and non-discriminatory (FRAND) terms if requested by the user.
   - The regulation pays particular attention to prohibiting unfair contractual terms relating to data sharing and use that have been unilaterally imposed between parties, thereby protecting SMEs.

3. **Stimulating the data market and increasing competition**

   The aim is to enable the creation of new, innovative data-driven services (e.g. predictive maintenance, repair services) through data sharing, thereby boosting the EU's overall economic performance.

4. **Facilitating switching between service providers (cloud switching)**

   The regulation facilitates switching between cloud and data processing service providers, thereby preventing vendor lock-in and increasing competition in this market.

2.1 Classification principles under the Data Act

Since the Data Act applies to products and services that are either "connected products" or "related services," we need to classify our products and services to determine whether this applies to us.

This can be done for each product and service by answering the questions in the table below.

If our answers match the content of the Connected Product or Connected Service column, we have identified a product or service to which the Data Act applies.

	Connected product	**Related service**
Is the product an object?	Yes	No
Does the product collect data on usage or environment?	Yes	-
Is the product capable of communicating data through physical access or a device?	Yes	-
Is the primary function of the product storage, transmission, or processing by a person other than the user?	No	-
The absence of the related service prevents one or more product functions from working.	Yes	Yes

2.2 Product classification according to the Data Act performed by Microsec zrt.

Microsec zrt. does not have any connected products.

Microsec Zrt. provides a related service for the e-Szignó Scan&Sign product, in which case it provides a related service for the scanner product that enables authentic conversion.

3 NIS2 Directive

NIS2 is an EU directive that strengthens cybersecurity requirements in approximately 18 sectors operating in critical sectors. Its aim is to achieve a uniformly high level of cybersecurity maturity in the EU by increasing the protection of networks and information systems, introducing stricter risk management requirements and incident reporting obligations.

This was incorporated into Hungarian legislation by **Act LXIX of 2024[4] on Hungary's cybersecurity** (hereinafter referred to as the Cybersecurity Act) and supplemented by detailed rules in **Decree MK 7/2024[5] on the requirements for security classification and the specific protective measures applicable to each security class** (hereinafter referred to as the MK Decree).

The Cybersecurity Act considers qualified trust services to be essential organizations under §1. (4) g), so the Microsec is required to perform a cybersecurity audit, which it publishes on its website.

3.1 Classification of information systems into security classes in accordance with the MK Decree

The classification of our electronic information systems into security classes shall be carried out in accordance with Section 2 of Annex 1 to the MK Decree.

[4] https://net.jogtar.hu/jogszabaly?docid=a2400069.tv

[5] https://net.jogtar.hu/jogszabaly?docid=a2400007.mkf

3.2 Classification of products and services into security classes in accordance with the MK decree, carried out by Microsec Ltd.

Classified into the **Basic security class**:

- All developed and distributed software products
  - e-Szignó Desktop
  - e-Szignó Mobile
  - e-Szignó SDK
  - e-Szignó Server
  - e-Szignó Autosigner Client| Service
  - e-Signature Preserver
  - e-Szignó Microsigner
  - e-Szignó Web On-Premise
  - e-Szignó Scan & Sign
  - e-Szignó Certmanager
- Services that fall outside the scope of trust services
  - Microsigner intermediary service
  - Eszosz

Classified into the **Significant security class:**

- Trust services
- V2X services

3.3 Additional guidance for supply chain risk management and control

NIS2 aims to protect the entire supply chain, so risk management must be extended to sub-contractors/suppliers and appropriate controls must be implemented.

It is recommended that Microsec Zrt. be audited in relation to supply management on the basis of the service provider's certifications.

Available conformity assessments/certifications:

- **eIDAS conformity assessment**

  Performed annually.

  A successful audit certificate proves (as these are prerequisites) that:

  - The service provider has an NIS2 audit.

    According to Article 21(2) of eIDAS, this is a prerequisite for the eIDAS conformity assessment of the service provider.

  - The service provider performs 4 vulnerability tests and 1 penetration test per year.

    This is mandatory under the Commission's implementing regulations.

  The eIDAS compliance assessment is available at:

  https://e-szigno.hu/eidas-certificates

- **NIS2 audit**

  This must be performed every two years.

  A successful audit certificate proves that the service provider complies with the NIS2 requirements.

  The NIS2 audit certificate is available at:

  https://www.microsec.hu/en/quality-assurance-and-audit

- **ISO 9001 and ISO 27001 certifications**

  These are renewed annually.

  The ISO 9001 and ISO 27001 certifications are available at the following link:

  https://www.microsec.hu/en/quality-assurance-and-audit

4 Dora Regulation

The DORA Regulation (Digital Operational Resilience Act) is an EU financial regulation that focuses on the operational resilience of the financial sector.

It sets rules and standards for financial institutions to detect, protect, recover from and repair information and communication technology incidents within financial institutions. Part of this regulation is to ensure that the activities of third-party ICT service providers (i.e. service providers who provide services to the financial institution) are monitored by the financial institution, so that it can be confident in the security of these service providers.

Third-party ICT service providers are subject to the provisions of Article 30 of the DORA Regulation.

4.1 Description of classification levels of the DORA regulation

To monitor the activities of third-party ICT service providers, the financial institution must classify them. There are three levels of classification, and they have different requirements:

4.1.1 Base

Unfortunately, DORA has not given a name to this category, but it will be referred to as the **Base** level in the following.

In this case, the contract with a third party must contain and comply with the provisions of Article 30(2) of the Regulation.

These are very brief:

- Full description of the service (documentation),
- Rules for the use of a subcontractor,
- Indication of the geographical location of the service,
- Data protection provisions,
- Provisions on the location of the service, the place of the service, the data protection provisions, the data return provisions,
- Obligation to cooperate with the authorities,
- Contract termination provisions,
- Obligation to participate in security awareness training of the financial institution.

4.1.2 ICT services supporting critical or important

By the definition of Regulation, the *'critical or important function' means a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorization, or with its other obligations under applicable financial services law;*

In the case of an ICT service supporting a critical or important function, the contract with a third party should include everything required at the Base level, plus two other essentials:

- The third-party ICT service provider must implement DORA-compliant business continuity plans and ICT security measures such as vulnerability scanning, penetration testing and code analysis.
- Participate in threat-based (TLPT) penetration testing.

4.1.3 Critical ICT third-party service provider

An ICT third-party service provider designated as critical in accordance with Article 31 by the relevant authority. There is none at the moment.

4.2 Development of the DORA classification methodology and classification

The classification of third-party ICT services shall be based on the methodology developed by the financial institution pursuant to Article 3(2) of 2024/1773/CID. This should be based on the following, taking into account the principles of risk management.

4.2.1 Proposed to classify as Base

All of the cases listed here are characterized by the fact that the substitution of the product/service by a market product can be ensured within a short time:

- Any service that is not integrated in use and has an alternative potential source.
- Services that are integrated with an open, standard interface

  For these, the standard interface allows the service to be transferred to an alternative provider supporting the same interface.
- Not custom-developed software.

The Base level classification can also be assisted by Article 30 1. and 2. of Commission Delegated Regulation (EU) 2017/565, which states:

> *1. For the purposes of the first subparagraph of Article 16(5) of Directive 2014/65/EU, an operational function shall be regarded as critical or important where a defect or failure in its performance would materially impair the continuing compliance of an investment firm with the conditions and obligations of its authorisation or its other obligations under Directive 2014/65/EU, or its financial performance, or the soundness or the continuity of its investment services and activities.*
>
> *2. Without prejudice to the status of any other function, the following functions shall not be considered as critical or important for the purposes of paragraph 1:*
>
> *(a) the provision to the firm of advisory services, and other services which do not form part of the investment business of the firm, including the provision of legal advice to the firm, the training of personnel of the firm, billing services and the security of the firm's premises and personnel;*
>
> *(b) the purchase of standardised services, including market information services and the provision of price feeds.*

On this basis, a number of services can be classified to Base level.

4.2.2 Proposed to classify as 'ICT services supporting critical or important functions'

In each of the cases listed here, it is not possible to replace the product/service with a market product quickly and in a short time:

- Any service that is not integrated with an open, standard interface when in use and would take longer to replace.
- Custom software (developed for the customer)

4.2.3 Why is it not recommended to classify anything at an unduly high level?

The argument against an unjustifiably 'critical or important' rating is that - compared to the Base level - it imposes the following requirements (to which resources must be allocated) on the financial institution:

- Article 28(8) requires that for services that support critical or important functions, the financial institution must also develop and implement exit strategies and that SHALL BE TESTED TOO.

In practice, this may mean that for an ICT system supporting a critical and important function, it may be necessary to obtain and test an equivalent service from another service provider in order to meet the conditions for migration to that service.

- - According to Article 29, ICT services supporting critical or important functions require an ICT concentration risk assessment and the implementation of appropriate control measures as a result.

4.3 DORA product classification carried out by Microsec Ltd. and recommended to its customers

To facilitate DORA compliance for its business customers, Microsec zrt. has carried out its own classification of its products/services according to DORA, which it recommends using.

The classification is shown in the table below.

Category	Group	Products
Base	Non-integrated services	Signing certificates Remote signing service with key management (e-Szignó Web or e-Szignó Mobile app interface) Seal certificates SSL certificates PSD2 certificates Time stamping Archiving OCCR
Base	Services integrated with an open, standard interface	Remote signing service, on CSC interface
Base	Non-custom developed software	e-Szignó Desktop e-Szignó SDK e-Szignó Server e-Szignó PDF Autosigner Microsigner Microsigner SDK e-Szignó Web on-premise MicroCA/MicroAC Suite e-Szignó Scan & Sign
ICT services supporting critical or important functions	Services not integrated with an open, standardized interface (Replacement would take longer.)	Remote signing service with key management with e-Szignó Web application (as signing interface) installed at the financial institution.

4.4 Additional guidance on preliminary risk assessment and due diligence under DORA

The financial institution is required to carry out a preliminary risk assessment under Article 5 of 2024/1773/CID and screening (due diligence) under Article 6 in relation to third party ICT service providers.

In order to facilitate these tasks, we have collected the answers to the pre-answerable questions on Microsec's fiduciary service in the table below.

In short:

for fiduciary services, we recommend to financial institutions to use our certifications as a result of third-party verification for risk assessment and due diligence.

Legislative section	Part to be examined	Answer	Justification
Article 5 (2) a)	[The risk assessment shall take into account all the risks …, including …] operational risks;	See Article 6 (1) b) and Article 5 (2) b)	-
Article 5 (2) b)	[The risk assessment shall take into account all the risks …, including …] legal risks;	The Service Provider, as a trust service provider, is obliged to have a liability insurance in accordance with Article 5 of Decree 24/2016 of the Ministry of Interior for the purposes described there and a financial guarantee for the risks related to the termination of the Service Provider in accordance with Articles 19-22.	As the audits/conformity assessments cover the testing of these requirements, it is recommended to use those documents to verify the compliance of the Service Provider with this requirement. See Article 6 (1) a) 2
Article 5 (2) c)	[The risk assessment shall take into account all the risks …, including …] ICT risks;	See Article 6 (1) b)	-

Legislative section	Part to be examined	Answer	Justification
Article 5 (2) d)	[The risk assessment shall take into account all the risks …, including …] reputational risks;	See Article 6 (1) a) 1	-
Article 5 (2) e)	[The risk assessment shall take into account all the risks …, including …] risks linked to the protection of confidential or personal data;	As a trust service provider, the Service Provider shall process, store and delete your data in accordance with the provisions of Section 88 (1) of the Digital Citizenship Act (DCA).	As the audits/conformity assessments cover the testing of these requirements, it is recommended to use those documents to verify the compliance of the Service Provider with this requirement. See Article 6 (1) a) 2
Article 5 (2) f)	[The risk assessment shall take into account all the risks …, including …] risks linked to the availability of data;	See Article 5 (2) e)	
Article 5 (2) g)	[The risk assessment shall take into account all the risks …, including …] risks linked to the location where the data is processed and stored;	Countries of data processing by the Service Provider: Hungary, Spain	The Privacy Notice includes this: https://www.microsec.hu/api/?func=cms.media&file=/pdf/microsec-privacy-notice-v1.14.pdf
Article 5 (2) h)	[The risk assessment shall take into account all the risks …, including …] risks linked to the location of the ICT third-party service provider;	The country in which the Service Provider is established: Hungary.	It can be checked in the Hungarian company register: https://www.e-cegjegyzek.hu/
Article 6 (1) a) 1	Has the business reputation,?	Yes, the Provider is 40 years old and has been providing trust services for more than 20 years.	https://www.microsec.hu/en/company-history

Legislative section	Part to be examined	Answer	Justification
Article 6 (1) a) 2	[Has] sufficient abilities, expertise and adequate financial, human and technical resources, information security standards, appropriate organizational structure, risk management and internal controls	The eIDAS and the Digital Citizenship Act (DCA) and the relevant standards explicitly impose requirements on the Service Provider in this respect, on the basis of which an annual compliance assessment is carried out. The Service Provider is also ISO 9001 and ISO 27001 certified. In addition, the Service Provider is further subject to NIS2 certification, which will be possible soon.	To verify the Service Provider's compliance with this requirement, it is recommended to check its annual certification documents, which are available in the following links: **eIDAS conformity assessment** https://e-szigno.hu/eidas-certificates **ISO 9001 and ISO 27001 certifications** https://www.microsec.hu/en/quality-assurance-and-audit **NIS2 certification** https://www.microsec.hu/en/quality-assurance-and-audit
Article 6 (1) a) 3	[Has] the required authorizations or registrations to provide the ICT services supporting the critical or important function in a reliable and professional manner;	The Service Provider is registered as a trust service provider with the NMIA (NMHH) (NMIA means National Media and Infocommunications Authority) The Service Provider is registered as a subject of the NIS2/Cybersecurity Act with the ASRA (SZTFH) (ASRA means Authority for the Supervision of Regulated Activities)	To verify the Service Provider's compliance with this requirement, it is recommended to check the records: **NMIA (NMHH)** https://esign.nmhh.hu/bszny/ **ASRA (SZTFH)** Currently no known searchable database online.

Legislative section	Part to be examined	Answer	Justification
Article 6 (1) b)	Has the ability to monitor relevant technological developments and identify ICT security leading practices and implement them where appropriate to have an effective and sound digital operational resilience framework;	The Service Provider is a trusted service provider committed to keeping abreast of technological developments. Trust services are required to have and test business continuity plans, as well as penetration and vulnerability testing.	As the audits/conformity assessments cover the testing of these requirements, it is recommended to use those documents to verify the compliance of the Service Provider with this requirement. See Article 6 (1) a) 2

5 Documentum revisions

Version	Date	Change
V1.0	2024-11-26	First version
V1.1	2024-12-03	Addition of products missing from the classification
V1.2	2025-05-21	Update
V1.3	2025-10-30	Addition of the NIS2 and the Data act