



**Velox**

Secure IT  
infrastructure

NIS2 SERIES · BOOKLET 1 OF 3

# NIS2

What every business leader needs to know  
about the new EU cybersecurity rules

1 · NIS2

2 · Implementation guide

3 · Incident response

# Contents

|           |                                        |    |
|-----------|----------------------------------------|----|
| <b>01</b> | Why NIS2 affects your business too     | 3  |
| <b>02</b> | Is your organisation in scope?         | 5  |
| <b>03</b> | The ten mandatory measures at a glance | 8  |
| <b>04</b> | <b>Technical measures in practice</b>  | 10 |
| <b>05</b> | Management accountability              | 15 |
| <b>06</b> | Incidents: what to report and when     | 16 |
| <b>07</b> | Supervision and penalties              | 18 |
| <b>08</b> | NIS2 in Bulgaria                       | 19 |
| <b>09</b> | What to do now                         | 21 |
| —         | Glossary                               | 22 |
| —         | Sources                                | 23 |
| —         | How Velox can help                     | 24 |

## About this booklet

A short introduction for managers and business owners. The next booklets in the series explain how to implement the measures and what to do when an incident happens.

# Why NIS2 affects your business too

---

Cyberattacks no longer hit only banks and large corporations. Ransomware brings factories, hospitals and municipal services to a halt, and attackers often get in through a smaller supplier with weaker defences.

## What NIS2 is

Directive (EU) 2022/2555, known as NIS2, is the common EU cybersecurity rulebook for organisations that the economy and society depend on. It replaced the first NIS Directive of 2016 and greatly widened the range of organisations it covers.

Member States had to bring it into national law by 17 October 2024. Bulgaria did so through amendments to its Cybersecurity Act adopted in early 2026.

**18**

sectors in scope

**10**

mandatory  
measures

**24 h**

to send the first  
notice

# What changes compared with the first directive

## 01 Many more sectors

Besides energy, transport and banking, it now covers food, waste, manufacturing, courier services and more.

---

## 02 A clear size threshold

As a rule, all medium-sized and large companies in these sectors are in scope.

---

## 03 The same minimum measures

Ten risk-management measures, mandatory across the EU.

---

## 04 Short reporting deadlines

24 hours, 72 hours and 1 month for significant incidents.

---

## 05 Accountability and higher fines

Management is personally accountable, and fines reach €10 million or 2% of worldwide turnover.

---

### THE KEY MESSAGE

Cybersecurity is now a duty of management, not just the IT department. Directors approve the measures, oversee their implementation and take training.

# Is your organisation in scope?

The first step is to find out whether NIS2 applies to you directly. Answer three questions:

- 1 Which sector are you in?**  
18 sectors in two annexes (page 6).
- 2 How large is your organisation?**  
As a rule, medium-sized and large companies.
- 3 Does an exception apply?**  
Some organisations are in scope whatever their size.

## What counts as medium-sized or large

### Medium-sized

50+ employees, or turnover and balance sheet above €10 million

### Large

250+ employees, or turnover above €50 million and balance sheet above €43 million

Linked and partner companies count too, for example within a group.

## In scope regardless of size

Providers of electronic communications, trust services, DNS and top-level domains; public administration; sole providers of an important service; organisations designated by the state.

# Sectors in scope

## Sectors of high criticality

Annex I · 11 sectors

|                                                  |                                 |
|--------------------------------------------------|---------------------------------|
| Energy                                           | Transport                       |
| Banking                                          | Financial market infrastructure |
| Health                                           | Drinking water                  |
| Waste water                                      | Digital infrastructure          |
| ICT service management<br>(business-to-business) | Public administration           |
| Space                                            |                                 |

## Other critical sectors

Annex II · 7 sectors

- Postal and courier services
- Waste management
- Manufacture and distribution of chemicals
- Production, processing and distribution of food
- Manufacturing: medical devices, computers and electronics, electrical equipment, machinery, motor vehicles and other transport equipment
- Digital providers: online marketplaces, search engines, social networks
- Research

**Note:** what counts is your actual activity, not the NACE code in the business register. A trader who delivers food to shops with its own fleet may fall under the Food sector.

# Essential and important entities

In-scope organisations fall into two groups. They differ in how they are supervised and in the size of the fines.

|              | Essential                                                                       | Important                                                                         |
|--------------|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Who they are | Large companies in Annex I sectors and certain organisations regardless of size | Everyone else in scope: medium-sized Annex I companies and all Annex II companies |
| Supervision  | Proactive: inspections and audits at any time                                   | Reactive: after a complaint or an incident                                        |
| Fines up to  | €10 million or 2% of worldwide turnover                                         | €7 million or 1.4% of worldwide turnover                                          |

The measures and reporting deadlines are the same for both groups. In Bulgaria, the final classification is made by the competent authorities (see chapter 8).

## NOT IN SCOPE? READ THIS

In-scope organisations must manage the risk that comes from their suppliers. If you provide them with IT, accounting, logistics or other services, expect questionnaires, new contract clauses and security requirements. Being well prepared is a competitive advantage.

# The ten mandatory measures at a glance

---

The directive requires appropriate and proportionate technical, operational and organisational measures that reflect the risks and the size of the organisation. We have grouped them for convenience. The letters match Article 21(2) of the directive.

### Organisational measures

---

rules, people, oversight

**(a) Risk and security policies**

Written rules on what is protected, against what, and who is responsible.

**(f) Assessing effectiveness**

Regular checks that the measures actually work.

**(g) Cyber hygiene and training**

Basic safe habits for everyone, and regular training.

**(i) Human resources security**

Rules for hiring, changing roles and leaving.

**Proportionality:** a small company does not need a bank's solutions, but it must cover all ten points at a scale that matches its risk.

## Operational measures

processes that run every day

### (b) Incident handling

How incidents are detected, contained and reported.

### (c) Business continuity

Backups, disaster recovery, crisis management.

### (d) Supply chain security

Requirements for suppliers and assessment of the risks they bring.

### (e) Security in acquisition, development and maintenance

Including vulnerability handling and disclosure.

## Technical measures

technologies and configuration

### (h) Cryptography and encryption

Protecting data at rest and in transit.

### (i) Access control and asset management

Everyone has only the access they need; you know what systems you have.

### (j) MFA and secured communications

Multi-factor authentication and secured communications, including in emergencies.

#### IN DETAIL

Chapter 4 covers the technical measures in practice. Full guidance on all measures is in Booklet 2, Implementation guide.

# Technical measures in practice

The directive does not name specific products. These are the typical solutions used to put the measures in place, with the letters of the measures they support.

---

|                                        |                |
|----------------------------------------|----------------|
| <b>Next-generation firewall (NGFW)</b> | <b>(e) (i)</b> |
|----------------------------------------|----------------|

Filters traffic by application and user, and stops attacks and malware.

---

|             |                |
|-------------|----------------|
| <b>SIEM</b> | <b>(b) (f)</b> |
|-------------|----------------|

Collects and correlates logs from all systems and detects suspicious activity.

---

|                          |                |
|--------------------------|----------------|
| <b>System monitoring</b> | <b>(b) (c)</b> |
|--------------------------|----------------|

Tracks the availability and health of servers, network and services, and raises an alert on failure.

---

|                                |                |
|--------------------------------|----------------|
| <b>Endpoint security (EDR)</b> | <b>(b) (e)</b> |
|--------------------------------|----------------|

Detects and stops attacks on computers and servers, not just known viruses.

---

|                                           |            |
|-------------------------------------------|------------|
| <b>Vulnerability and patch management</b> | <b>(e)</b> |
|-------------------------------------------|------------|

Regular scanning and timely fixing of security holes.

---

|                                  |                |
|----------------------------------|----------------|
| <b>Access management and MFA</b> | <b>(i) (j)</b> |
|----------------------------------|----------------|

Central accounts, role-based permissions, secure remote access (VPN).

---

|                          |            |
|--------------------------|------------|
| <b>Protected backups</b> | <b>(c)</b> |
|--------------------------|------------|

Copies outside the main network that ransomware cannot alter.

---

# The network: the first line of defence

(e) (i) (j)

Most attacks come in through the network: from the internet, through remote access or from a device inside that is already infected.

## Next-generation firewall (NGFW)

Recognises applications and users, not just addresses. Blocks known attacks (IPS), filters dangerous websites and scans files for malicious code. The router from your internet provider is no substitute.

## Network segmentation

Separate zones for the office, servers, guests, cameras and other IoT devices, and production. An infected laptop should not be able to reach the accounting server.

## Secure remote access

VPN with multi-factor authentication for every user. No Remote Desktop (RDP) exposed to the internet.

## Wireless network

A separate guest network. For staff: individual accounts (WPA2/WPA3-Enterprise) instead of a shared password.

### THE MINIMUM FOR A SMALL ORGANISATION

An NGFW with active security subscriptions, at least three network segments, VPN with MFA, and no management interface reachable from the internet.

# People and devices

(b) (i) (j)

Most breaches start with a stolen account or an infected computer.

## MFA everywhere

Email, VPN, cloud services and above all administrator accounts. Where possible, use phishing-resistant methods (an authenticator app with number matching, or a FIDO2 key) instead of SMS.

## Separate administrator accounts

Day-to-day work is done with a standard account; the privileged one is used only when needed. Everyone has the minimum rights their job requires.

## Endpoint security (EDR)

Traditional antivirus is no longer enough. EDR watches how computers and servers behave, detects unknown attacks and can automatically isolate an infected device.

## Mobile device management (MDM)

Encryption, locking and remote wipe for company phones and laptops.

## Email security

Filtering against phishing and malicious attachments, plus SPF, DKIM and DMARC to stop others spoofing your domain.

### THE MINIMUM

MFA on every service reachable from outside, EDR on every computer and server, and no administrator rights for everyday work.

## Visibility: knowing what is going on

(b) (f)

The 24-hour deadline assumes you will notice an incident in time. Without logs and monitoring, attacks are often discovered weeks later.

### System monitoring

Continuous checks on servers, network devices, internet connections and backups, with an alert to the person responsible when something fails.

### Central event logging

Logs from the firewall, servers, cloud services and accounts are collected in one place, protected from tampering and kept long enough for an investigation.

### SIEM

Analyses the logs and connects events that look unrelated: failed logins, a sign-in from an unusual country, a spike in outbound traffic. That is how it spots attacks no single system can see.

### Alerts from EDR

Endpoint security (previous page) feeds its alerts into the SIEM, so you get the full picture.

For digital and managed IT service providers, Implementing Regulation (EU) 2024/2690 explicitly requires monitoring and event logging.

#### WHO IS WATCHING THE ALERTS?

Tools only help if someone responds. For small organisations, the most realistic option is to outsource monitoring as a managed service.

# Resilience: recovering from an attack

(c) (e) (h)

## The 3-2-1-1-0 backup rule

3 copies of your data, on 2 different media, 1 off-site, 1 immutable or offline, and 0 errors in test restores.

## Test your restores

A backup that has never been restored is only a hope. Test regularly, for example once a quarter.

## Know your RTO and RPO

How quickly each system must be back up (RTO), and how much data you can afford to lose (RPO).

## Vulnerabilities and updates

A complete inventory of devices and software. Critical updates go in within days, not months, including on the firewall and VPN. Regular vulnerability scanning.

## Encryption

Encrypted disks on laptops and mobile devices, and secure connections (TLS) everywhere.

**Technology alone is not compliance.** You also need policies, accountable people and regular reviews that everything works.

# Management accountability

NIS2 puts cybersecurity in the hands of management bodies (Article 20 of the directive). It cannot be handed over entirely to the IT department or an outside provider.

### Approves

the risk measures

### Oversees

their  
implementation

### Answers

for infringements

## Mandatory training

In Bulgaria, members of management bodies must take cybersecurity training at least once every two years. They must also arrange regular training for staff.

## Personal liability

Where they are personally at fault, managers face fines of €500 to €5,000. At essential entities that ignore supervisory orders, managers can be temporarily banned from management roles.

### IN PRACTICE

Cybersecurity is a standing item on the board agenda, with decisions, budget and reports.

# Incidents: what to report and when

### When an incident is "significant"

When it has caused, or could cause, severe disruption to services or financial loss for the organisation, or considerable damage to others. Only significant incidents must be reported.

## The deadlines

The clock starts when you become aware of the incident.

**24 h**

### Early warning

Whether malicious action is suspected and whether other countries could be affected.

**72 h**

### Incident notification

Initial assessment: severity, impact, indicators of compromise.

**On request**

### Intermediate report

A status update, if the authority asks for one.

**1 mo.**

### Final report

Root cause, measures taken, cross-border impact.

## Where to report

- To the sectoral incident response team (sectoral CSIRT), as set out in the Cybersecurity Act.
- If personal data is affected, also to the data protection authority (CPDP) within 72 hours under the GDPR.
- Where needed, also inform customers affected by the incident.

## First steps when you suspect an incident

- 1 Isolate, don't switch off.** Disconnect affected devices from the network, but don't power them down or delete anything.
- 2 Notify the person responsible** and your IT provider.
- 3 Write down** what you noticed, when and how.
- 4 Decide whether it is significant.** If so, the 24-hour deadline is already running.
- 5 Don't pay a ransom** or contact the attackers without expert advice.

### IN DETAIL

The full plan, with roles, contacts and notification templates, is in Booklet 3, Incident response.

# Supervision and penalties

Supervisory authorities can carry out inspections and audits, demand information and evidence, issue binding instructions and make infringements public.

## Fines for organisations in Bulgaria

|                                                       | Essential  | Important   |
|-------------------------------------------------------|------------|-------------|
| Maximum                                               | €10M or 2% | €7M or 1.4% |
| Minimum for breaching the measures or reporting rules | €25,000    | €12,500     |

The percentage is of worldwide annual turnover; whichever amount is higher applies.

- Ignoring a binding instruction: €2,500–12,000, or €5,000–25,000 for a repeat offence.
- Personal fines for managers: €500–5,000 (see chapter 5).
- If personal data leaks, a GDPR penalty may follow as well.

**The fine is often not the biggest cost.** A halted business, lost data and lost customer trust cost more.

# NIS2 in Bulgaria

Bulgaria transposed the directive through the Act amending and supplementing the Cybersecurity Act, published in the State Gazette, issue 17 of 13 February 2026.

## Key dates

|                    |                                                                                           |
|--------------------|-------------------------------------------------------------------------------------------|
| <b>17 Feb 2026</b> | Amendments in force; measures and reporting apply from this date                          |
| <b>1 Jun 2026</b>  | End of the 50% reduction in penalties                                                     |
| <b>17 Aug 2026</b> | Deadline for the decision on sectoral authorities and the method for identifying entities |
| <b>17 Oct 2026</b> | Deadline for the updated ordinance on minimum requirements                                |
| <b>17 Nov 2026</b> | Deadline for a new national cybersecurity strategy                                        |

**As of October 2026**, some of the secondary legislation is still pending. Watch for changes: dates and authorities may still be clarified.

# Who does what

## **Sectoral competent authorities**

Decide which organisations are essential or important, using a method set by the Council of Ministers, and supervise their sector.

---

## **Register of entities**

Not public; kept at national level. You must report changes to your details (name, address, contacts, IP ranges) within two weeks.

---

## **Incident response teams (CSIRTs)**

Sectoral teams (SERIKS) receive incident reports. The national team (NERIKS) coordinates at national level.

---

## **CPDP**

The Commission for Personal Data Protection, when an incident involves personal data.

---

### **DON'T WAIT FOR A LETTER**

The obligations on measures and reporting already apply. If you think you are in scope, start preparing now rather than waiting to hear from the authority.

# What to do now

---

Seven steps any organisation can start on this month:

- ☐ **Check your scope.** Sector, size, exceptions (chapter 2).
- ☐ **Appoint someone responsible** and put the topic on the management agenda.
- ☐ **Map your systems and data** and carry out a first risk assessment.
- ☐ **Close the quick gaps:** MFA, tested backups, updates (chapter 4).
- ☐ **Prepare an incident plan** with roles and contacts for the 24-hour deadline.
- ☐ **Train management and staff.**
- ☐ **Review your suppliers** and your contracts with them.

**BOOKLET 2**

Implementation guide

**BOOKLET 3**

Incident response

# Glossary

**Business continuity** — the ability to keep operating during and after an incident.

**Competent authority** — the public body that supervises a given sector.

**CSIRT** — computer security incident response team; in Bulgaria, sectoral teams (SERIKS) and a national team (NERIKS).

**Cyber hygiene** — basic safe habits: strong passwords, updates, watching out for phishing.

**Early warning** — the first notice of a significant incident, within 24 hours.

**Essential entity** — an in-scope organisation with proactive supervision and the highest fines.

**Important entity** — an in-scope organisation with reactive supervision and lower maximum fines.

**MFA** — multi-factor authentication: signing in with at least two factors, such as a password and a code on your phone.

**Ransomware** — malicious software that encrypts your data and demands a ransom.

**Risk management** — identifying, assessing and reducing risks to your systems.

**Significant incident** — an incident with serious impact on services, finances or other people; it must be reported.

**Supply chain** — the suppliers of products and services your organisation depends on.

**Vulnerability** — a weakness in a system or software that can be exploited in an attack.

# Sources

## LEGISLATION

Directive (EU) 2022/2555 (NIS2), 14 December 2022

[eur-lex.europa.eu/eli/dir/2022/2555/oj](https://eur-lex.europa.eu/eli/dir/2022/2555/oj)

Commission Implementing Regulation (EU) 2024/2690

[eur-lex.europa.eu/eli/reg\\_impl/2024/2690/oj](https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj)

Act amending and supplementing the Bulgarian Cybersecurity Act, State Gazette No. 17 of 13 February 2026 (in Bulgarian)

[dv.parliament.bg](https://dv.parliament.bg)

## OFFICIAL GUIDANCE

European Commission, NIS2 Directive

[digital-strategy.ec.europa.eu/en/policies/nis2-directive](https://digital-strategy.ec.europa.eu/en/policies/nis2-directive)

ENISA, the EU Agency for Cybersecurity

[www.enisa.europa.eu](https://www.enisa.europa.eu)

Bulgarian Commission for Personal Data Protection

[www.cdpd.bg](https://www.cdpd.bg)

## STANDARDS

ISO/IEC 27001:2022, Information security management systems

[www.iso.org/standard/27001](https://www.iso.org/standard/27001)

Information is current as of October 2026. This booklet is for information only and is not legal advice. Pending secondary legislation may clarify the requirements.



## How Velox can help

Velox designs, builds and supports IT infrastructure for businesses. We help organisations move from "we need to do something" to concrete measures that work.

### Readiness assessment

Scope, current state and a list of gaps.

### Technical measures

NGFW, SIEM, system monitoring, MFA, backups.

### Subscription support

Ongoing care for your systems, updates and monitoring.

### For suppliers

Getting ready for requirements from customers covered by NIS2.

**GET IN TOUCH**

**[www.velox-systems.com](http://www.velox-systems.com)**

**[office@velox-systems.com](mailto:office@velox-systems.com)**

## NIS2 SERIES

Three short booklets for leaders who want to understand NIS2 and act on it.

- 1 · NIS2
- 2 · Implementation guide
- 3 · Incident response



**Velox**

Secure IT  
infrastructure

[www.velox-systems.com](http://www.velox-systems.com)  
[office@velox-systems.com](mailto:office@velox-systems.com)

© 2026 Velox Ltd. For information only; not legal advice.