ESET Digital Security
Progress. Protected.

EVERSHEDS SUTHERLAND

NIS2

Get ready for the EU's newest cybersecurity legislation

Co-Authors:
Saranda Walgaard
Andre Lamerias

TABLE OF CONTENTS

What is NIS2?

NIS2 creates a new scope to strengthen the level of cybersecurity across the EU. This updated version of the first Network and Information Systems Directive entered into force on 16 January 2023, requiring entities operating in critical sectors such as energy, transport, health, digital services, and managed security services to implement improved risk management. NIS2 also introduces new reporting rules and fines.

NIS vs. NIS2: The evolution of EU cybersecurity regulation

The NIS directive, adopted in 2016, was the first legislation on cybersecurity concerning all member states of the European Union. It mainly focused on organisations in two groups: operators of essential services (OESs), such as health, transport, energy, etc., and digital service providers (DSPs), including online search engines, internet marketplaces, and cloud services. NIS required these organisations to comply with appropriate security measures and report any major cybersecurity incidents they experience, but the directive also enabled the states to consider their national circumstances.

NIS2 creates a new scope to strengthen the level of cybersecurity across the EU. This updated version of the first Network and Information Systems Directive entered into force on 16 January 2023 and will include not only the member states of the EU but also organisations outside the EU that are essential within its market. Enterprises classed as “High Criticality” will be required to take both technical and operational measures to comply with NIS2, including **incident response, supply chain security, encryption and vulnerability disclosure, adequate risk analysis, testing and auditing of cybersecurity strategies, and crisis management planning in view to ensure business continuity**. In case of a cyber incident, these entities will also be required to submit an initial notification within 24 hours and more detailed information within 72 hours. NIS2 also introduces fines for failure to comply, including suspension of certification and personal liability to managerial positions, in line with national laws.

Which sectors were included in the NIS Directive?

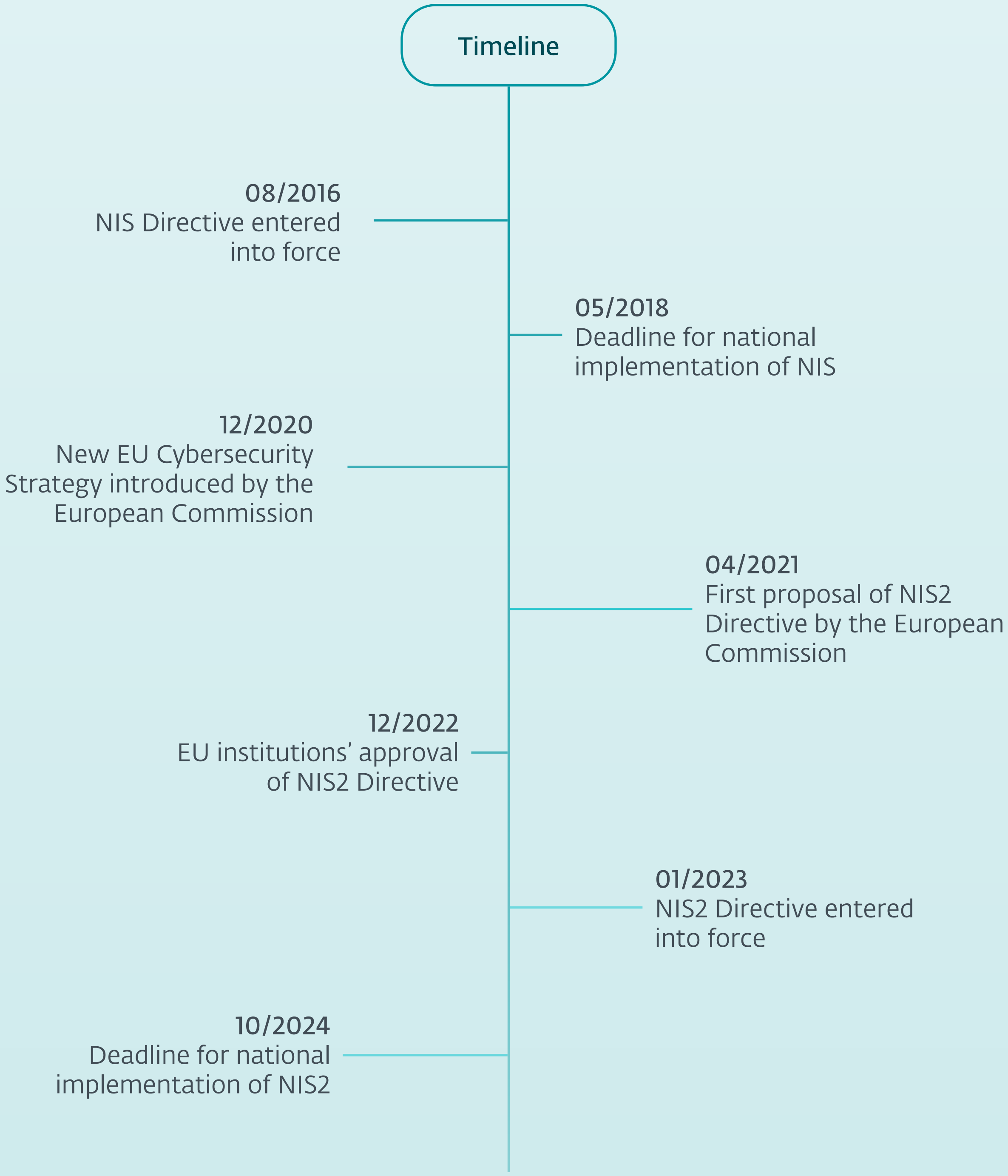
- Healthcare
- Digital infrastructure
- Transport
- Water supply
- Digital service providers
- Banking and financial market infrastructure
- Energy

Which sectors were added by the NIS2 Directive?

- Providers of public electronic communications networks or services
- Wastewater and waste management
- Manufacturing of certain critical products (e.g., pharmaceuticals, medical devices, and chemicals)
- Food
- Digital services (e.g., social networking platforms and data centre services)
- Space (e.g., aerospace)
- Postal and courier services
- Public administration

The Directive also establishes **the European Cyber Crises Liaison Organisation Network**, EU-CyCLONe, to enable cooperation between national agencies and authorities in charge of cybersecurity, and each member state will also be required to clearly identify a single point of contact to report cyber incidents.

The NIS2 will become applicable after the EU member states transpose the Directive into their national law: by September 2024. Nevertheless, organisations might want to be ready sooner rather than later, not only to be timely on the implementation process, but also to test different good practices on incident handling, control policies and reporting mythologies.



Timeline

08/2016
NIS Directive entered into force

05/2018
Deadline for national implementation of NIS

12/2020
New EU Cybersecurity Strategy introduced by the European Commission

04/2021
First proposal of NIS2 Directive by the European Commission

12/2022
EU institutions' approval of NIS2 Directive

01/2023
NIS2 Directive entered into force

10/2024
Deadline for national implementation of NIS2

Who needs to comply?

Compared to its previous version, the new NIS Directive eliminates the distinction between operators of essential services and digital service providers: entities would be classified based on their importance, and divided into two categories: essential and important entities, which will be subjected to different supervisory regimes.

It means that **all sectors and organisations coming under NIS2 are of great importance to communities within the European Union. It is understood that their disruption would cause serious harm to society if they were no longer able to execute their functions.** Ultimately, the two categories were created to distinguish the fact that not all sectors impact society at the same scale in the event of an incident.

Which industries are involved?

Essential Entities (EEs)

large operators from sectors of **high criticality** and special cases.

Large-sized organisation threshold

> 250 employees
> 50 M€ turnover
> 43 M€ balance

Sectors of high criticality

- Energy
- Transport
- Banking
- ICT service management
- Drinking water
- Wastewater
- Health care providers
- Digital infrastructure
- Public administration
- Financial market infrastructure
- Space

Important Entities (IEs)

large operators from other critical sectors and **medium-sized operators**.

Medium-sized organisation threshold

50 - 250 employees
10 - 50 M€, turnover
< 43 M€ balance

Other critical sectors

- Post and courier
- Waste management
- Manufacture, production and distribution of chemicals
- Manufacture, production and distribution of food
- Manufacturing (electronics and other)
- Digital providers
- Research

Both entity types have the same duties and obligations, e.g., members of the management bodies of essential and important entities are required to follow training and must take appropriate and proportionate technical, operational, and organisational measures to manage the risks posed to the security of network and information systems. Entities use these for operations or the provision of services to prevent or minimise the impact of incidents on recipients of their or other services.

Essential organisations will also be required to have a proactive preparedness framework to evaluate the impact of mismanagement even without an incident. For important entities, compliance is expected reactively, meaning these organisations will only be checked for compliance with laws and requirements after an incident. Should it be concluded that insufficient action was taken and requirements were not met, sanctions apply to both types of entities.

It is important to note that by 17 April 2025, and every two years after that, the competent authorities shall notify the Commission and the Cooperation Group of the number of essential and important entities for each sector.

Duty of care and duty to report

All organisations covered by NIS2 — essential or important — will have to start complying with their duty of care. The Directive contains a list of types of measures that service providers must comply with as a minimum. These include risk assessment to check whether an organisation pays sufficient attention to information systems security, crisis management, and operational continuity in the event of a major cyber incident and can ensure the security of their supply chain. Further, the duty of care includes ensuring the security of network and information systems, using cryptography and encryption, and having policies and procedures that assess the effectiveness of risk management measures. The duty to report will also apply to all organisations covered by NIS2. This reporting obligation will require affected organisations to notify their national authorities within 24 hours of becoming aware of an incident, followed by a 72-hour update and a final assessment one month after.

The duty of care

Under the former NIS Directive, the duty of care applies to both essential and digital service providers. It involves taking appropriate and proportionate technical and organisational measures to manage the risks to the security of network and information systems.

The new NIS2 Directive establishes a different distinction: essential and important entities, reflecting the extent to which they are critical as regards their sector or the type of service they provide, as well as their size. Both types of entities will be required to comply with the duty of care. It is up to the member states to establish a list of essential and important entities based on the most appropriate national mechanisms, allowing entities to register themselves. Entities become subject to cybersecurity risk management measures when registered under one of the two categories. These should be proportionate to the degree of the essential or important entity's exposure to risks and to the societal and economic impact that an incident would have. Due account of the entity's criticality, size, and likelihood of occurrence of incidents should also be taken.

In this context, security refers to the ability of network and information systems to withstand actions that compromise availability, authenticity, integrity, and confidentiality. The Commission Implementing Regulation (Regulation (EU) 2018/151) further specifies the security elements to be observed: security of systems and facilities, incident handling, business continuity management, monitoring, control and testing, and international standards.

The NIS2 Directive lists a minimum set of measures, including conducting risk analysis and instituting policies on information systems security, incident enforcement, business continuity and crisis management, supply chain security, and security in the procurement, development, and maintenance of network and information systems. Also included are policies and procedures to assess the effectiveness of risk management measures and the use of cryptography and encryption.

Essential and important entities **should also adopt a wide range of basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness; organise training for their staff; and raise awareness concerning cyber threats, phishing, or social engineering techniques**. Furthermore, those entities should reevaluate their cybersecurity capabilities and, where appropriate, pursue the integration of cybersecurity-enhancing technologies, such as artificial intelligence or machine-learning systems, to enhance their capabilities and the security of network and information systems.

In addition, to demonstrate compliance with these measures, **member states may require essential and important entities to use specific ICT products, services, or processes that will be certified under the European cybersecurity certification schemes** adopted under the Cybersecurity Act (Regulation (EU) 2019/881).

Moreover, the European Commission is empowered to adopt implementing and delegated acts to specify risk management measures further. Thus, obligations can become more defined, taking into account new cyber threats, technological developments, or sector-specific features.

The duty to report

With the advent of the NIS2 Directive, in addition to the duty of care, the duty to report, which already existed under the original NIS Directive, will be fleshed out.

Under the first NIS Directive, a duty to report incidents that significantly impact service continuity was introduced. According to the Directive, an incident is said to occur when there is "any event with an actual detrimental effect on the security of network and information systems". Security refers to "the ability of network and information systems to withstand actions that affect the availability, integrity, confidentiality, and authenticity of network and information systems with a certain degree of reliability". **To assess whether an incident has significant impact, the guideline describes several parameters to be considered, including the number of users affected, the duration of the incident, and the size of the geographical area affected by the incident**. If, for a supplier, an incident appears to have a significant impact on the continuity of the service provided, the incident **must be reported without delay to the local Computer Security Incident Response Team (CSIRT) or competent authority as designated by the member state**. The report's content must contain sufficient information to enable the competent authority or the CSIRT to determine the cross-border impact of the incident.

The NIS2 Directive provides for a "two-stage approach" to incident reporting. The first notification aims to limit the potential spread of incidents and to allow entities to seek support. The second reporting should be thorough, ensuring that lessons can be learned from previous incidents. It is important to note, however, that further clarifications might be required to clearly assess the incident and its consequences. In addition, it also aims to gradually improve the resilience of individual companies and entire sectors to cyber threats.

Incidence reporting stages according to NIS2

Within 24 hours of becoming aware of the incident (and without undue delay) a first notification should be made to the competent authority or the nationally relevant CSIRT. If possible, it should indicate whether an unlawful or malicious act caused the incident. This provision satisfies the strictly necessary information.

Within 72 hours from the first alert, the affected entity is required to submit an update and initial assessment with more detail on the attack and measures put in place. If requested by the entity, it is possible to receive guidance on implementing potential mitigation measures and, if required, additional technical support. In the case of a criminal incident, the impacted entity also receives guidance on reporting the incident to law enforcement authorities.

Within one month of the submission of the first notification, a final report must be submitted, including:

- a detailed description of the incident, its severity and consequences
- the type of threat or cause likely to have led to the incident
- applied and ongoing mitigation measures

The provision regarding reporting incidents with significant consequences has been adopted in the NIS2 Directive, adding that **entities will also have to report any major cyber threat they identify that could lead to a significant incident**. Regarding the term “cybersecurity,” it follows the definition laid down in the Regulation on ENISA (the European Union Agency for Cyber Security) and on Certification of Cyber Security of Information and Communication Technology — the Cybersecurity Act. This regulation defines cybersecurity as “the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats“. An incident is considered significant if the incident results or may result in significant operational disruption or financial losses for the entity concerned or if the incident has affected or may affect natural or legal persons by causing significant material or immaterial damage.

Entities outside the scope of the NIS2 Directive may voluntarily report significant incidents, cyber threats, or near misses. The competent authority or CSIRT shall follow the procedure described under the “two-stage notification”. Voluntarily submitted reports may not be subject to any additional obligations. Thus, if an entity makes a voluntary notification, it should not be subject to more onerous obligations than if it had not submitted it.

How is it going to work?

It is up to the member states to carry out effective supervision to ensure compliance with the requirements of NIS2 once they implement it into their national legislation.

Regarding essential entities, this implies proactive supervision. In contrast, it implies reactive supervision for important entities, which **may be triggered by evidence, indication, or information that the entity allegedly does not comply with the Directive**. Indeed, in the latter case, action should only be taken when, for a member state, it appears that an important entity does not comply with the obligations laid down in the Directive.

	Essential Entities (EEs)	Important Entities (IEs)
Supervision regime:	Proactive	Reactive
Non-compliance penalties:	up to 10 million euros or up to 2% of the total annual worldwide turnover	up to 7 million euros or up to 1,4% of the total annual worldwide turnover

For definition of EEs and IEs, see table on page 5.

The measures taken by competent authorities must be effective, proportionate, and dissuasive. For both types of entities, **the competent bodies will have the power to subject them to on-site inspections and off-site ex-post supervision conducted by trained professionals, targeted security audits, security scans, requests to access data, documents and information, and requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence**. Random checks further expand the list together with ad hoc audits in the case of essential entities. Except for duly substantiated cases, the audited entities will need to bear the costs of the security audits.

If an infringement is discovered, the competent authorities can exercise further enforcement powers, such as issuing warnings, adopting instructions, ordering entities to cease conduct of activities that infringe on the Directive, ordering entities to inform the natural or legal persons that may be affected by the misconduct, or even making the information public. Should these measures not lead to remedying the situation, the competent authorities may temporarily suspend the entity’s activities and the organisation’s manager, who is discharging responsibilities at a chief executive or representative legal level.

The NIS2 Directive sets up a consistent framework for sanctions across the Union, by establishing a minimum list of administrative sanctions for breach of the cybersecurity risk management and reporting obligations. These sanctions include binding instructions, implementing the recommendations of a security audit, bringing security measures in line with NIS2 requirements, and administrative fines.

Member states must provide the relevant authorities the ability to impose considerable fines. Regarding essential entities, it is a maximum of at least €10,000,000 or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Concerning important entities, a maximum fine is set to €7,000,000, or at least 1,4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Management bodies of essential and important entities may also be held liable for non-compliance with the provisions of the NIS2 Directive. If your organisation is a covered entity and fails to build and maintain cyber-fitness, there will be fines and penalties for non-compliance with risk management measures or reporting obligations.

To strengthen the supervision that helps ensure effective compliance, the NIS2 Directive provides a minimum list of supervisory means through which competent authorities may supervise essential and important entities. These include regular and targeted audits, on-site and off-site checks, information requests, and document or evidence access.

When exercising their enforcement powers, competent authorities should give due regard to the particular circumstances of each case, such as the nature, gravity, and duration of the infringement, the damage caused or losses incurred, and the intentional or negligent character of the violation.

To ensure accountability for the cybersecurity measures at the organisational level, **NIS2 introduces provisions on the liability of natural persons holding senior management positions** in the entities falling within the scope of the new NIS2 Directive.

What does NIS2 mean for small and midsized businesses?

NIS2 establishes the application of the size-cap rule, as defined in the table on page 5. While it excludes the majority of small and midsized businesses from having to comply with the new rules, some exceptions apply — for example, for **SMBs in the sectors of electronic communications networks or publicly available electronic communications services, trust service providers or top-level domain (TLD) name registries**.

SMBs are increasingly becoming the target of supply chain attacks due to limited security resources. Such supply chain attacks can have a cascading effect on entities to which they provide supplies. **Member states should, through their national cybersecurity strategies, help SMBs to address the challenges faced in their supply chains**. Member states should have a point of contact for SMBs at the national or regional level, which either provides guidance and assistance to SMBs or directs them to the appropriate bodies for guidance and assistance with regard to cybersecurity-related issues.

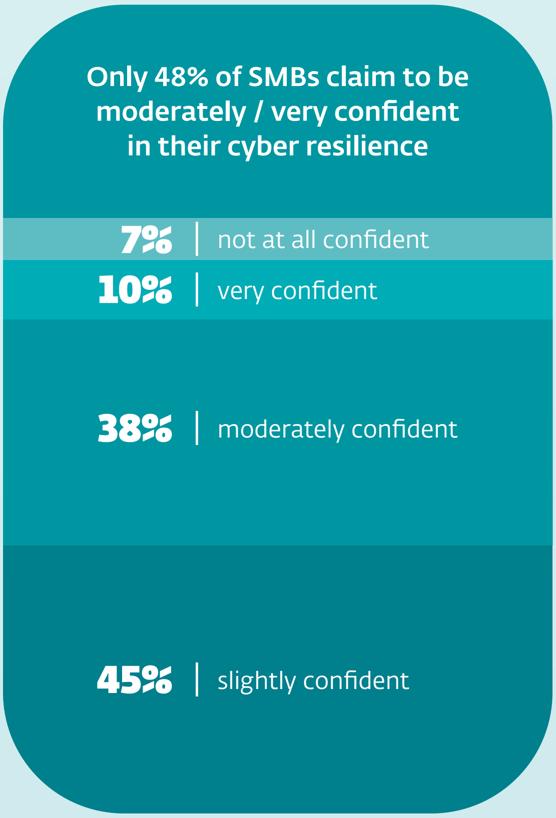
i

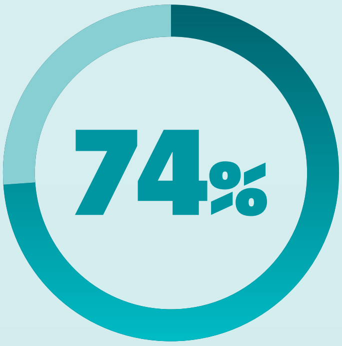
In March last year, the European DIGITAL SME Alliance, EU's largest SME network in the field of ICT, published its position paper to the consultation on the proposal for NIS2, welcoming the new Directive, but also alerting for the indirect impact of NIS2 on SMBs.

According to James Philpot, Project Manager at DIGITAL SME, **the first step SMBs should be taking to understand specific needs to boost their cybersecurity practices is looking at their national cybersecurity centre and ENISA's guides and recommendations**. However, it might be easier or harder to get the right information as different member states provide different resources. Nonetheless, NIS2 mandates that the states should provide support and resources mainly when it comes to getting a detailed understanding of the scope of this legislation and whether their customers will be subject to it, which will help plan ahead.

“Downstream suppliers are likely to be the most disrupted, and it can be challenging for some companies to have the needed technical capabilities but mainly to understand reporting requirements and how NIS2 interplays with other legislation”, explained Philpot.

SMBs confidence in cyber resilience


Only 48% of SMBs claim to be moderately / very confident in their cyber resilience



74% of SMBs believe that businesses of their size are more vulnerable to cyberattacks than large enterprises

Source: ESET SMB’s Digital Security Sentiment Report (2022)

Generally speaking, any efforts to improve the level of cybersecurity in European businesses should be welcomed. Moreover, DIGITAL SME as well as ESET are convinced that this new framework might be an opportunity. The only caveat, alerts Philpot, is the level of implementation and support, and how that is managed will ultimately be the difference between the legislation helping SMBs and the legislation being regulatory overburden.

SMBs can reach out to their local CSIRTs to mitigate some of the deficiencies of other national bodies, or take advantage of resources such as the DIGITAL SME/SBS guide, the DIGITAL SME Guide on Information Security Controls or cybersecurity certificates.

SMBs top concerns over the business implications of a cyberattack

29%	loss of data
23%	financial impacts
18%	loss of customer confidence and trust
16%	operational disruption
13%	reputation damage

Source: ESET SMB's Digital Security Sentiment Report (2022)

As Philpot also notes in the conversation with ESET, the impacts of cyber incidents are well known to SMBs: data leaks, considerable financial impact and loss of customer confidence. In the very least, they can take the NIS2 Directive as an opportunity to develop greater awareness and strengthen their cyber resilience.

Follow Digital Security Guide by ESET for digital security tips for small and midsized businesses

ESET®

Digital Security
Progress. Protected.

For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defences in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centres worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and Twitter.

EVERSHEDS
SUTHERLAND

Eversheds Sutherland is a global law and civil-law notary firm with 74 offices in 35 countries and employs more than 3,000 lawyers. Due to our international character, we are able to provide cross-border advice like no other. In Europe, Eversheds Sutherland has 44 branch offices.

This handbook was created with the support of ESET Government Affairs.