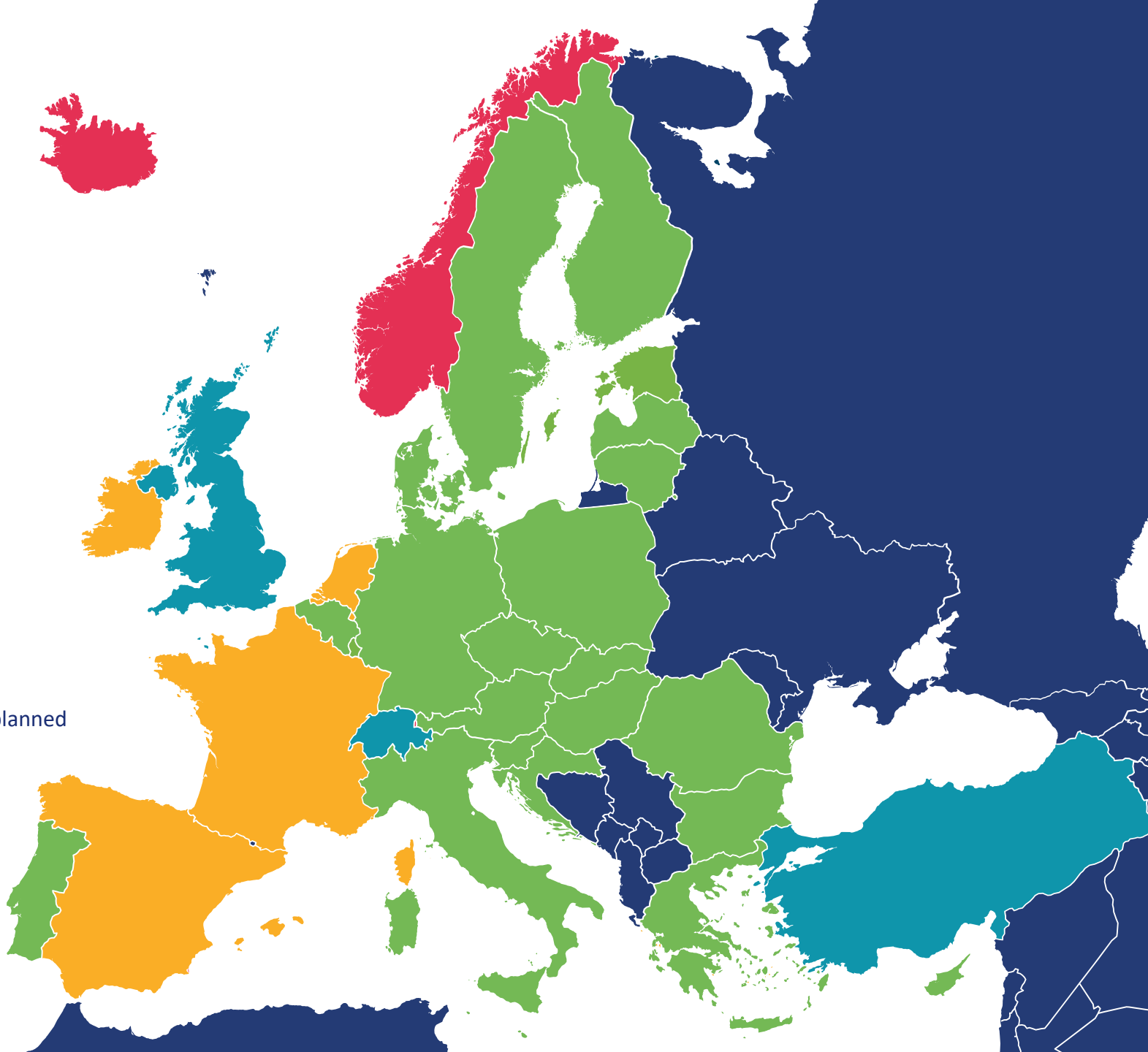
fieldfisher

NIS2 across the EU

Which countries have implemented the NIS2 Directive into local law?

- Implemented
- Draft Published
- No Draft
- Similar regime in force or planned



Accurate as at 25 June 2026

NIS 2 across the EU

Under NIS2, Member States must have notified ENISA by **17 January 2025** of the in-scope entities providing certain digital services in their territory.

This is a key deadline in the Member States that have already transposed their law, as they have required various digital services providers to register prior to this deadline.

We have been assisting clients with registration across the EU. **Contact us if you have not yet registered and our team can support you to register quickly, in compliance with local requirements.**

The deadline for transposition set in the directive expired on **17 October 2024.** The EU Commission has initiated **infringement proceedings** against a number of EU Member States, in response to the continuing delay in implementing the NIS2 Directive.

This includes:

- the countries that had not yet implemented NIS2 in time; and
- the countries whose local laws may not fully comply with NIS2 (e.g. Latvia and Hungary).

Key changes: Among other features, NIS2:

- significantly widens the scope of entities and sectors that will be regulated for cyber security;
- imposes much more prescriptive requirements on cyber security risk-management compared to other legislation like the GDPR; and
- sets out new enforcement measures which could have significant impacts on management bodies.

Current implementation status: In collaboration with our relationship firms across the EU, our market-leading European Cybersecurity team is delighted to have produced this NIS2 status update. Many states have missed the 17 October 2024 deadline to implement the Directive into local law, with several not even expecting to be ready until Q2 or Q3 of 2025.

Also, it currently looks like the EEA countries of Norway, Iceland and Liechtenstein will implement NIS2 although this may still take several years.

What next? Businesses operating or providing services in the EU need to assess if they are in scope of NIS2, what they need to do to comply and where they will need to register. These are not simple questions and different thresholds and tests apply to determine what local laws are relevant.
This is particularly important for digital service providers who may be able to benefit from the Article 26 main establishment principle, potentially simplifying their compliance requirements.

How to get in touch. If you would like to receive updates on new developments or would like to speak with our cybersecurity legal experts, please contact
Julia Spurrett:
julia.spurrett@fieldfisher.com

Fieldfisher Cybersecurity Team

Our multidisciplinary Cyber team works across the Fieldfisher network, advising on all issues around cyber-security and defence. We focus on areas as diverse as policies, cyber readiness and training, regulatory compliance, breach containment, insurance, mergers and acquisitions, litigation and regulatory outreach and defence.

We are particularly well versed in the range of new digital regulation coming into force across the UK and EU, including the Digital Operational Resilience Act (DORA), NIS2, the AI Act and other regimes focused on telecoms security and connected devices.

We have a pan-European network of offices and relationship firms with whom we are collaborating to bring you this status update and help with client queries in each Member State. Please see below for our key contacts on NIS2 in each Member State.

James Walsh
Partner, Technology, London

+44 (0) 330 460 7083
james.walsh@fieldfisher.com

Kirsten Whitfield
Partner, Data, London

+44 (0) 330 460 7058
kirsten.whitfield@fieldfisher.com

Michael Butterworth
Director, Data, London

+44 (0) 330 460 6122
michael.butterworth@fieldfisher.com

Country status and key contacts

Austria

Implemented

Philipp Reinisch
philipp.reinisch@fieldfisher.com

Not yet in force: NISG 2026, the implementing act, was published on 23 December 2025. It will enter into force on 01 October 2026.

Belgium

Implemented

Tim Van Canneyt
tim.vancanneyt@fieldfisher.com

Olivier Proust
olivier.proust@fieldfisher.com

Bulgaria

Implemented

Mariya Papazova
m.papazova@ppgllawyers.eu

Irena Georgieva
i.georgieva@ppglawyers.eu

Croatia

Implemented

Boris Dvoršćak
boris.dvorscak@ilej-partners.com

Cyprus

Implemented

Demetris Gregoriou
demetris.gregoriou@neo.law

Andrea Kallis
andrea.kallis@neo.law

Czech Republic

Implemented

Robert Nešpůrek
robert.nespurek @havelpartners.cz

Dalibor Kovář
dalibor.kovar@havelpartners.cz

Guidance was published on 04 May 2026 which clarifies the scope of the Cybersecurity Act on branches of foreign companies. In April 2026, the NUKIB simplified the NIS2 registration process by creating a single unified form – "Notification and management of regulated services" which is available on the NUKIB Portal.

Denmark

Implemented

Bodil Hald
bmh@plesner.com

Niels Christian Ellegaard
nce@plesner.com

Estonia

Implemented

Ants Nomper
ants.nomper@ellex.legal

Merlin Liis-Toomela
merlin.liis-toomela@ellex.legal

Finland

Implemented

Martin von Willebrand
martin.vonwillebrand@hhpartners.fi

Anna-Sofia Toivettula
anna-sofia.toivettula@hhpartners.fi

There are several Finnish legislative updates. The Act on the Cyber Resilience of Certain Products and Cybersecurity Certification allows information sharing between market surveillance and NIS2 supervisory authorities. Amendments to the Act on Electronic Communications Services extend its scope to entities acting on behalf of domain name registrars and introduce provisions covering non-Finnish top-level domains. Changes to the Cybersecurity Act expand CSIRT responsibilities and permit disclosure of information to the Financial Supervisory Authority. Additionally, a Government Proposal seeks to extend military intelligence assistance obligations to data centre service providers under the Cybersecurity Act.

France

Draft Published

Anne-Laure-Hélène des Ylouses
alhdesylouses@fieldfisher.com

The bill on the resilience of critical infrastructure and the strengthening of cybersecurity, which transposes the European NIS2 directives into French law, has still not been adopted. The planned date is July 2026.

Country status and key contacts

Germany

Implemented

Martin Lose
martin.lose@fieldfisher.com

Thorsten Ihler
thorsten.ihler@fieldfisher.com

Greece

Implemented

Dr Nikos Th. Nikolinakos
nikolinakos@nllaw.gr

Dina Kouvelou
kouvelou@nllaw.gr

Hungary

Implemented

Zsombor Orbán
orban.zsombor@provaris.hu

Claudia Bagoly
Bagoly.claudia@provaris.hu

On 11 June 2026, SZTFH Decree No. 6/2026 (8.VI.) came into force which simplifies the requirements for cybersecurity auditors. Under the new regime, all auditors must meet uniform conditions regardless of the cybersecurity classification of the systems they audit reducing the administrative burden on businesses.

Ireland

Draft
Published

Leonie Power
leonie.power@fieldfisher.com

Italy

Implemented

Diego Rigatti
diego.rigatti@fieldfisher.com

Paola la Notte
paola.lanotte@fieldfisher.com

Latvia

Implemented

Sarmis Spilbergs
sarmis.spilbergs@ellex.legal

Mikijs Zimecs
mikijs.zimecs@ellex.legal

Lithuania

Implemented

Jaunius Gumbis
jaunius.gumbis@ellex.legal

Tomas Kamblevicius
tomas.kamblevicius@ellex.legal

Luxembourg

Implemented

Ingrid Dubourdieu
ingrid.dubourdieu @fieldfisher.com

Errol Briones
errol.briones@fieldfisher.com

The Luxembourg NIS2 Law A225 entered into force on 10 May 2026, along with Law A226 implementing the RCE Directive. Registration is required by 10 July 2026.

Malta

Implemented

Andrew Zammit
andrew.zammit@gvzh.mt

Nick Scerri
nick.scerri@gvzh.mt

"Measures for a High Common Level of Cybersecurity across the European Union (Malta) (Amendment) Order, 2026": recently implemented to provide a more formal enforcement mechanism; designate the Malta Information Technology Agency as the national CSIRT; coordinate vulnerability disclosure, strengthen the independence of cybersecurity audits, refine the governance of the National Cyber Security Steering Committee and update the sectors and categories of entities and designated competent authorities.

Netherlands

Draft
Published

Ady van Nieuwenhuizen
ady.vannieuwenhuizen @fieldfisher.com

Merel van Aar
merel.vanaar@fieldfisher.com

The House of Representatives has adopted the draft legislation for NIS2 implementation. In parallel, the government is working on the underlying secondary legislation. The government continues to aim for simultaneous entry into force of NIS2 and the related secondary legislation, although it has missed its own deadline of Q2 2026.

Country status and key contacts

Norway

No Draft

Selmer

Stale Hagen
s.hagen@selmer.no

Jennifer Parmlind
j.parmlind@selmer.no

Norway has adopted the Digital Security Act to implement the NIS1 Directive, with the Act entered into force on 1 October 2025.

Poland

Implemented

fieldfisher

Marcin Huczkowski
Marcin.Huczkowski@fieldfisher.com

Bartosz Jussak
Bartosz.Jussak@fieldfisher.com

The NIS 2 legislation entered into force on 3 April 2026.

Portugal

Implemented

CRA
COELHO RIBEIRO E ASSOCIADOS

Mónica Oliveira Costa
monica.costa@cralaw.com

Jaime Medeiros
jaime.medeiros @cralaw.com

The Cybersecurity Legal Framework Regulation (Regulation 756/2026) entered into force on 23 June 2026, and the registration function on the MyCiber portal is now available. In-scope organisations are required to register via the portal within 60 days of it becoming available (for entities operational as at 3 April 2026), or within 30 days of commencing operations where they begin operating after that date.

Romania

Implemented

NNDKP
Legal & Tax

Iurie Cojocaru
iurie.cojocaru@nndkp.ro

Oana Stefan
oana.stefan@nndkp.ro

On 17 June 2026, Romania's DNSC issued two draft orders. 1) establishing a comprehensive framework for authorising, monitoring, and revoking cybersecurity training providers. 2) Updating a prior draft, introducing mandatory cybersecurity risk management measures for entities classified as Essential or Important. It defines three assurance levels Basic, Important, and Essential with cumulative compliance requirements and introduces a standardised methodology for assessing the maturity of cybersecurity measures.

Slovakia

Implemented

HAVEL & PARTNERS
CONNECTED THROUGH SUCCESS

Štěpán Štarha
stepan.starha@havelpartners.sk

Adam Klizan
adam.klizan@havelpartners.sk

Slovenia

Implemented

karanovic/partners

Kevin Rihtar
kevin.rihtar@karanovicpartners.com

Spain

Draft
Published

fieldfisher

Carlos Pérez
carlos.perez@fieldfisher.es

Sweden

Implemented

ADVOKATFIRMAN FYLGIA

Martin Gynnerstedt
martin.gynnerstedt@fylgia.se

Regulations on incident reporting and information obligations by the Swedish Civil Defence Authority ("MCF") enter into force on 1 July 2026. The regulations are called "MCFFS 2026:8; Myndigheten för civilt försvars föreskrifter om incidentrapportering och informationsskyldighet för väsentliga och viktiga verksamhetsutövare".

Switzerland

Similar regime in force or planned

NKF

Clara-Ann Gordon
clara-ann.gordon@nkf.ch

Switzerland is subject to a separate bi-lateral trade agreement with the EU and has been pursuing its own reforms with various similar features to NIS2. A new requirement for operators of critical infrastructure to report cyber attacks within 24 hours of discovery became effective on 1 April 2025; penalties for reporting violations apply from 1 October 2025.

Türkiye

Similar regime in force or planned

BTS&PARTNERS

Melis Mert
melis.mert@bts-legal.com

Yasin Beceni
yasin.beceni@bts-legal.com

Türkiye's new Cyber Security Law, in force since 19 March 2025, establishes a national framework for protecting digital infrastructure and regulating cyber operations. It imposes compliance obligations on public and private entities, including incident reporting, inspections, and oversight of cyber-sector M&A. Secondary legislation will refine these duties, with partial alignment to the EU's NIS2 Directive expected.

UK

Similar regime in force or planned

fieldfisher

James Walsh
james.walsh@fieldfisher.com

Michael Butterworth
michael.butterworth @fieldfisher.com

On 1 April 2025, the UK government announced further details on the proposed Cyber Security and Resilience Bill which will update the UK's existing NIS Regulations in several key areas.