RÖDL

We pave the way.
Worldwide.

roedl.com

Newsletter
IP, Privacy & Compliance

January 2026

Northern Strength
Trusted Expertise in the Nordic-Baltic Region

Read in this issue:

Denmark

EU AI Act Update: What changes lie ahead?

An overview of the current status and potential changes to the EU AI Act

The EU AI Act: What has happened so far?

When the European Union's Artificial Intelligence Act (the EU AI Act) entered into force on 1 August 2024, it was described as ground-breaking legislation as it established the world's first comprehensive legal framework for regulating AI. The EU AI Act aims to ensure that there are clear guidelines for the development of responsible AI and that human rights are respected.

The EU AI Act has introduced a risk-based approach covering the entire AI value chain (from providers to distributors, importers and deployers). The risk-based approach entails that the requirements for an AI system will depend on the level of risk associated with the use of the AI system - the higher the risk, the more stringent the requirements. The EU AI Act classifies AI systems in the following four main categories; prohibited AI practices, high-risk systems, limited-risk systems with transparency duties, and minimal-risk systems that face no additional obligations beyond existing law. The EU AI Act sets out the requirements that must be met for an AI system to fall into the various categories.

The EU AI Act has introduced a phased implementation, meaning that the provisions in the Act will enter into force gradually at specific milestones. The early provisions entered into force in 2025.

Below is a timeline containing the current key milestones of the EU Act:

Date:	**Milestone:**
1 August 2024	The EU AI Act officially enters into force and becomes legally binding across the EU.
2 February 2025	Prohibitions on certain AI practices as determined in article 5, and AI literacy requirements enter into force. Prohibitions include, among others, manipulative AI, social scoring, and certain biometric systems and categorization.
2 August 2025	Provisions for providers of general-purpose AI models (GPAI) enter into force. Moreover, provisions on governance structures, confidentiality and most sanctions for non-compliance also enter into force.
2 August 2026	Core requirements for high-risk AI systems as defined in article 6(2) and as listed in Annex III enter into force (see exception below) in conjunction with the rest of the AI Act.

2 August 2027	The requirements for systems classified as high risk as they are covered by specific parts of other EU harmonization legislation (in particular product safety rules) as defined in article 6(1) and listed in Annex I enter into force.

Potential changes to the EU AI Act:

Based on the timeline provided above, 2026 should mark a new phase of the EU AI Act, as the core requirements for high-risk AI systems, such as AI systems used in recruitment and credit scoring, should enter into force. High-risk AI systems are the core of the EU AI Act.

However, on 19 November 2025 the European Commission published a Digital Omnibus Package, in which the Commission proposed to postpone the entry into force of provisions concerning the core requirements for high-risk AI systems from 2 August 2026 until supporting measures such as harmonized standards, common specifications, and Commission guidelines are available. The requirements for core high-risk systems will then apply 6 months after the Commission's confirmation. In any case, the core high-risk AI requirements will apply no later than 2 December 2027.

Moreover, the Commission has also proposed extending certain simplifications to small mid-cap companies (e.g., simplified technical documentation, proportionate fines and tailored guidance), and replacing the AI literacy obligation for providers and deployers with a general duty for the EU and Member States to promote AI literacy. For deployers of high-risk AI systems, the stringent requirements will remain in place. Under current law, the AI literacy requirement entails an obligation for both providers and deployers of AI systems to implement measures to ensure a sufficient level of AI literacy of staff and other persons involved in the operation and use of AI systems.

At this stage, the Digital Omnibus Package is only a proposal from the Commission and has been submitted to the European Parliament and the Council for further consideration. Any amendments will take legal effect only once adopted by the Council and Parliament. In the meantime, the current regulations and timelines in the EU AI Act will apply.

Recommendations

As the proposed amendments have not yet entered into force, it is our recommendation that companies should only adjust their existing implementation timelines once the changes have been adopted. In the meantime, companies should prepare and establish internal compliance structures to ensure compliance with the EU AI Act.

As a basic starting point, we recommend the following process:

1. Map the AI usage and identify the types of AI systems that are currently used within the company and determine whether they can be categorized as prohibited AI practices, high-risk systems, limited-risk systems with transparency duties or minimal-risk systems, and assess whether the requirements are met.
2. Gain technical and organizational insight into how each AI system works and is used.
3. Implement policies and procedures, and train staff in AI ethics, compliance, and responsible use.
4. Stay updated on EU AI Act developments and guidance.

Contact in Denmark

Navina Jegarubanathan

Advokat | Attorney-at-Law

T +45 60 52 43 04
navina.jegarubanathan@lead-roedl.com
www.lead-roedl.dk

Finland

Comprehensive reform of Data Protection Act by the end of 2026

Finland is preparing a major revision of its data protection legislation[1], expected by late 2026. The aim is to streamline data use in public services while keeping privacy protections strong.

Outdated or overly restrictive rules that hinder lawful data use, data sharing, or cloud services are likely to be revised, with the aim of making fuller use of the GDPR 's[2] flexibility. The reform is still in preparation, and no final bill has been passed yet, but the goal is a clearer, more consistent framework for authorities, businesses, and citizens.

Why is this amendment necessary?

Rules on personal data processing are scattered across many sector-specific laws adopted over decades. Some are outdated, overlapping, or hard to interpret together. This fragmentation increases administrative burden, complicates information exchange, and slows digital service development. Organizations also need to apply several layers at once, including GDPR, the national Data Protection Act, and information management requirements, which can create uncertainty and inconsistent practices.

What is the aim of this initiative?

1. Clarity and predictability

A central objective is to make the choice of legal basis more predictable in daily work. The reform aims to provide clearer guidance on when processing rests on legal obligation, public interest, exercise of official authority, or consent.

The reform also targets secondary use of data. Information collected for one service may later be needed for service development, research, or statistics. The goal is to make it easier to assess when broader use is permitted and what safeguards are required.

---

[1] Finland's Data Protection Act (1050/2018)
[2] The EU General Data Protection Regulation (GDPR, Regulation (EU) 2016/679)

2. Security and safeguards

The amendment highlights high risk processing, especially sensitive data such as health information or criminal records. The direction is toward practical, risk-based assessments of necessity and proportionality and clearer expectations on safeguards when risks to individuals are significant. It also seeks workable protection in public data services to balance openness with privacy.

3. Streamlined digital services and data flows

A third theme is reducing operational friction created by accumulated sector rules. The reform is expected to review outdated or duplicative provisions that slow service delivery or impose rigid transfer procedures. The intent is to rely more consistently on GDPR principles and the national Data Protection Act, and to simplify electronic transfers, so lawful information exchange can happen smoothly when a valid basis exists.

Cloud services are central to this work. The revision intends to clarify expectations for international transfers and multi provider service chains through clearer approaches to risk assessment, contracts, and safeguards.

4. Accountability and enforcement

Shared digital services often involve multiple actors, which can make compliance responsibilities unclear. The reform is considering ways to make roles and responsibilities clearer, supporting transparency for individuals and more predictable operations for organizations. Oversight and enforcement are also under review, including options for stronger supervision and, in some cases, administrative fines for authorities.

Summary – Practical angles for SMEs

Finland's planned update of the Data Protection Act points toward clearer rules, smoother data use, and more predictable compliance. While details are still developing, SMEs should expect greater emphasis on risk-based assessments, accountability, and digital-ready processes.

1. Public–private data transfers: Contracts and workflows involving authorities may need closer attention, particularly around data-sharing arrangements, roles, and transfer mechanisms.
2. Cloud services: EU/EEA and cross-border transfer requirements are likely to remain a key focus, with contractual and technical safeguards continuing to play an important role.
3. Sector-specific impacts: Developments may affect industries differently, potentially requiring updates to documentation, internal controls, and data-handling practices as new rules emerge.

Taken together, these areas point to the value of early impact assessments and well-timed updates to contracts and internal processes. Our team is closely monitoring the reform and can support SMEs in preparing for the new requirements as they develop.

Contact in Finland

Nora Haapala

Attorney-at-Law
Associate Partner

M +358 40 66 55 011
nora.haapala@roedl.com
www.roedl.fi

Latvia

Compliance is not a box-ticking exercise – it is a core risk-management function

Why internal rules matter even when the law seems obvious

“Everyone is presumed to know the law.” This fundamental principle – ignorantia legis non excusat – underpins all modern legal systems. In theory, it means that individuals and companies alike are responsible for complying with applicable laws, even if they are unaware of them. From this perspective, one might ask: why repeat legal prohibitions in internal policies at all, if the law is already clear? The answer lies not in formal compliance, but in risk allocation.

Employment Changes the Legal Equation

Employment relationships are not neutral contractual arrangements. Across the EU and EEA, they are governed by the assumption that the employee is the weaker party, while the employer bears a heightened duty of care. At the same time, employees are presumed to act in the name and in the interests of the employer. As a result, unlawful conduct by an employee may trigger civil, administrative or even criminal liability for the employer, particularly where authorities or courts conclude that the company failed to ensure adequate supervision, guidance or preventive measures.

This logic is firmly rooted in the long-established principles of culpa in eligendo (fault in selecting employees) and culpa in instruendo (fault in instructing, training and supervising them). In practice, this means that liability is often shifted from the individual employee to the company, while the employer’s theoretical right of recourse against the employee is frequently limited or illusory.

Why Liability Outcomes Are Inherently Unpredictable

In disputes involving employee misconduct, courts and authorities do not look at a single rule in isolation. Instead, they assess complex factual and organizational structures, including:

1. how employees were instructed and trained,
2. whether risks were foreseeable,
3. how information flowed internally,
4. whether escalation mechanisms existed and were used, and
5. whether management exercised effective oversight.

Because these assessments are highly fact-specific, outcomes are often difficult to predict, particularly in cross-border EU/EEA contexts where multiple legal regimes, authorities and enforcement standards may intersect. What may appear to be a “clear case” on paper can quickly evolve into a high-stakes, multi-layered dispute with significant financial and reputational exposure.

Compliance as Prevention, Not Formality

Against this background, internal compliance rules serve a purpose that goes far beyond discipline or box-ticking.

Well-designed internal policies and training programs perform three critical functions:

1. Preventive – helping employees recognize legally sensitive situations before violations occur;
2. Guidance-based – clearly defining expected conduct, decision-making paths and escalation channels;
3. Evidentiary – demonstrating that the employer exercised due care, potentially limiting or excluding liability under culpa in instruendo.

Importantly, authorities increasingly ask not whether rules exist, but whether they are understood, implemented and applied in practice.

A Practical Reality Check

Experience shows that simply asking employees to “acknowledge” policies is rarely sufficient. Employees may overlook key provisions, misunderstand legal risks or fail to recognize red flags in real-life situations.
Just one real life example – a sales employee – aiming to meet commercial targets – coordinated pricing behavior with online retailers and facilitated the buy-out of parallel imports to maintain market prices. The employee did not perceive this as problematic. For the company, however, the consequences included serious competition law violations, reputational damage and multi-million-euro fines.

The lesson is clear: compliance is not about legal theory, but about operational awareness.

A Shared EU/EEA Logic – and a Clear Business Conclusion

While enforcement thresholds differ, the underlying principles – employer responsibility, heightened duties of care, and the relevance of culpa in eligendo / instruendo – are largely harmonized across the EU and EEA countries.

Where employee’s conduct can expose a company to fines (sometimes up to 10% of turnover), criminal sanctions or civil claims, investing in a living compliance system is not a cost burden, but a rational risk-management decision. In most cases, prevention is significantly cheaper – and far more predictable – than defending complex disputes after the fact.

Each company should therefore assess its specific risk profile, identify areas requiring internal regulation and training, usually, internal policies should address employee conduct in key legal areas, including in particular: (i) personal data processing and privacy, (ii) cybersecurity, (iii) protection of confidential information, (iv) identification and protection of company know-how, (v) intellectual property created by employees and use of third-party IP (software, images, music, etc.), (vi) conflicts of interest, (vii) gifts, hospitality and other benefits, including anti-corruption aspects, (viii) competition law, fair commercial practices and comparative advertising, (ix) AML, KYC and export control compliance. Besides, the company must ensure that compliance mechanisms are not merely documented, but actively embedded in day-to-day operations. Because when things go wrong, it is not only the law that will be examined – but everything the company did, or failed to do, beforehand. Prevention is almost always less costly than dealing with the consequences.

Contact in Latvia

Inese Kalnāja

Senior Counsel | IP, Competition and Compliance

T +371 67338125
inese.kalnaja@roedl.com
www.roedl.lv

Lithuania

The Data Act: Is Lithuania ready?

In December 2023, the European Parliament and the Council adopted a new piece of legislation applicable to EU Member States - Regulation 2023/2854, also known as the Data Act. This Regulation entered into force on January 11, 2024.

Most of the rights and obligations provided for in the Data Act became applicable on September 12, 2025, while some provisions, such as those relating to changes in product design and manufacturing or unfair contract terms, will apply on September 12, 2026, and September 12, 2027, respectively.

Thus, what is the Data Act and to which areas does it apply?

The Data Act is an EU regulation adopted in response to the ever-increasing amounts of data generated globally and within the EU each year, which, according to the drafters of the legislation, has until now been "locked up" in the hands of digital product manufacturers or service providers and largely inaccessible to the general public. This regulation is relevant for companies that manufacture or sell internet-connected products and data (cloud) service providers. Its purpose is to ensure fair and transparent data exchange practices and to enable both individuals and businesses to access and control the data generated by their network-connected devices. Under Data Act, companies must ensure that data is accessible to consumers and enable a smooth change of service provider. Here it is important to understand the essence – under the Data Act, the user will have full access to the data generated using a product or service and will be able to decide what to do with these data.

Areas of application of the Data Act:

- Data generated by Internet-connected products. Determines who can use and access it in all sectors of the economy in the EU;
- Provision of data to public sector authorities for exceptional needs (in the event of emergencies);
- Change of data (cloud) management services. The aim is to protect companies from unfair contractual terms related to data sharing imposed by stronger players;
- Data interoperability. The aim is to ensure that data can move smoothly between sectors and Member States.

Are you properly prepared for the application of the Data Act?

Now that we are entering the fifth month since the Data Act began to be applied in practice, it is time to check whether preparations for the implementation of this regulation have been carried out properly and whether anything has been overlooked in doing the groundwork. Thus, have you:

- created a data map?
- implemented data sharing processes?
- created export buttons?
- reviewed your contracts?
- coordinated your Data Act implementation actions with your privacy and security teams?

If you have not yet taken the above steps or have only done so partially, now is the time to focus on what remains to be done and take a firm step towards full implementation of the Data Act. Take actions to:

- identify personal and non-personal data, products, and services covered by the Data Act;
- find out what exemptions might apply to your situation so you can refuse to provide access to data and protect your business;
- identify possible grounds for refusal, implement measures to protect trade secrets, and put in place processes to respond to consumer inquiries;
- implement access based on design and default features in smart products and related services;
- adapt unilateral data sharing terms to avoid invalidation and implement transparency requirements;
- include privacy and security teams in the compliance process to ensure an integrated approach to GDPR and cybersecurity requirements.

Obligations of Member States under the Data Act

The Data Act is a directly applicable EU document, which means that there is no need to adopt additional national legislation – it directly grants rights and imposes obligations on natural and legal persons, therefore, individuals can rely on it and demand the enforcement of their rights in national courts, even if national law does not provide for this. However, the Data Act contains several areas that require Member States to complement the regulation with national laws and regulations.

First, the Data Act requires that Member States appoint one or more competent authorities supervise the compliance with the Data Act – handle complaints and have the power to conduct investigations and impose administrative fines that are effective, proportionate and dissuasive. In Lithuania, the Lithuanian Communications Regulatory Authority (in Lithuanian – Lietuvos Respublikos ryšių reguliavimo tarnyba) is expected to be designated as the competent authority.

Moreover, under the Data Act, Member States had until September 12, 2025, to establish effective, proportionate, and dissuasive sanctions and the necessary measures to ensure that sanctions are enforced. Unfortunately, we must admit that this has not yet been done in Lithuania, but it is expected that legislation to remedy these shortcomings will be adopted in the summer of 2026.

Conclusion

In summary, it should be noted that for users, the Data Act is a cause for celebration, but for businesses, it means a lot of homework. Whether you are a manufacturer, service provider, or user, the Data Act will affect you in one way or another – its impact on Lithuanian business will be real. It is therefore necessary to respond to the fact that the act has already begun to be applied and to prepare for its scope to be expanded in the future. Let's take the necessary steps together!

Contact in Lithuania

Laima Nevarauskaitė

Senior Associate | Assistant Attorney

T +370 5 212 35 90
laima.nevarauskaite@roedl.com
www.roedl.lt

Norway

Intellectual Property in the age of AI: A Norwegian perspective

Creativity, Technology and the Limits of Existing IP Law

Artificial intelligence and generative technologies are reshaping how creative and innovative works are produced. While the core legal definition of intellectual property (IP) has not changed, its application has become significantly more complex. Copyright, patent and related IP regimes were developed on the assumption that creative and inventive activity is carried out by humans. Generative AI challenges this assumption by producing outputs that resemble human-created works, raising difficult questions about authorship, ownership and legal responsibility.

For Norway, a digitally advanced economy closely integrated with the European Union through the EEA Agreement, these questions are not theoretical. Norwegian businesses, creators and public authorities increasingly rely on AI tools while remaining bound by national IP law and harmonised European rules.

AI-Generated Content and Authorship

Under Norwegian copyright law (åndsverkloven), as under EU copyright law, protection is reserved for works created by a natural person and reflecting individual creative choices. Content generated entirely by an AI system, without meaningful human creative input, does not qualify for copyright protection. This position is well established in both legislation and case law and applies regardless of the economic value of the output.

Where AI is used as a tool, copyright protection may arise only if a human exercises sufficient creative control. Minimal actions, such as entering a short or generic prompt, will normally not meet this threshold. More substantial involvement - for example, developing detailed instructions, selecting between outputs, or editing the result creatively - may give rise to protection for the human contribution, but not for the AI-generated elements as such.

Training Data and Copyrighted Works

One of the most significant IP challenges posed by generative AI concerns the use of copyrighted material in training datasets. Training typically involves copying and analysing large volumes of data, which may include protected works. Under EU copyright law, which is relevant for Norway through the EEA framework, text and data mining of lawfully accessible works is permitted unless rights holders have expressly reserved their rights. This exception applies irrespective of whether the use is commercial or non-commercial.

However, lawful training does not permit the generation of outputs that reproduce protected works verbatim or in a substantially similar form. The distinction between permissible training and infringing output remains critical and requires careful assessment in practice.

Responsibility for Infringing Outputs

AI systems themselves cannot hold rights or bear legal responsibility. If AI-generated content infringes IP rights, responsibility will lie with human actors. Users may be liable where they exercise creative control or use outputs without appropriate review. Developers may face responsibility where infringement results from how systems are designed, trained or deployed, or where safeguards are inadequate. In many cases, contractual arrangements between developers, users and customers will play a decisive role in allocating risk and liability.

Norway and the European Regulatory Context

Norway does not have AI-specific IP legislation. Instead, IP issues related to AI are addressed through existing copyright, patent and contract law, supplemented by harmonised European rules that apply through the EEA Agreement. The EU Artificial Intelligence Act introduces transparency and compliance obligations for certain AI systems, including requirements related to copyright, but it does not create new IP rights or alter the fundamental principles of authorship.

Norwegian authorities are expected to interpret and enforce these rules within existing institutional frameworks, alongside established IP bodies and courts.

Ethical and IP-Conscious AI Use

For Norwegian organisations, ethical AI use requires recognising that AI is a tool and that responsibility remains with the user. Outputs should always be reviewed before use or dissemination. Uploading confidential or proprietary materials into external AI systems may amount to unauthorised disclosure and can violate IP and confidentiality obligations.

Risk mitigation measures include using professional AI services with clear contractual safeguards, understanding how data is processed, and adopting internal policies governing acceptable AI use. In a high-trust legal and commercial environment, maintaining respect for intellectual property is essential to sustaining confidence in AI-driven innovation.

Conclusion

AI does not replace the foundations of intellectual property law, but it exposes their limits. For Norway, the challenge lies in enabling innovation while preserving the human-centred principles that underpin IP protection. Careful interpretation, contractual clarity and responsible use - rather than radical legal redesign - remain the most reliable tools in the age of generative AI.

Contact in Norway

Anniken Ramse

Partner | Attorney-at-Law

T +47 917 11 517
ara@seland-roedl.no
www.seland-roedl.no

Sweden

NIS 2 – The New Cybersecurity Law

As of January 2026, the new Cybersecurity Act (2025:1506) will be implemented in Sweden

In 2022, the EU adopted Directive (EU) 2022/2555, known as the NIS 2 Directive, to strengthen cybersecurity across the Union. This directive updates Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, replaces Directive (EU) 2016/1148 (the NIS Directive), and aims to ensure a higher, more uniform level of cybersecurity in an increasingly digital society. As of 15 January 2026, the NIS 2 Directive will be implemented in Swedish law through the new Cybersecurity Act (2025:1506). The Cybersecurity Act will replace the Act (2018:1174) on information security for critical and digital services, which was based on the previous NIS Directive.

What is the purpose of NIS 2 and the new Cybersecurity Act?

Both the Cybersecurity Act and the NIS 2 Directive aim to achieve an overall high level of cybersecurity in society, all across the EU. The Act will regulate the obligation of public and private operators to take measures to protect their network and information systems, as well as the obligation to report significant incidents. Furthermore, the Cybersecurity Act will regulate the supervision and intervention options for operators who fail to comply with the provisions of the Act. Finally, certain amendments are proposed to other Acts concerning electronic communications, top-level domains and confidentiality.

Scope of application – private, public and non-profit sectors

NIS 2 and the Cybersecurity Act cover the private, public and non-profit sectors. Within the private sector, the Act is primarily aimed at medium-sized and large companies. The main rule is that companies with more than 50 employees or EUR 10 million in annual turnover are covered by the Act. However, it is important to note that corporate group structures are taken into account, meaning that a company may itself fall below the thresholds, but can still be covered by the regulations due to its affiliation with a corporate group. If, for example, a parent company falls within the thresholds, all affiliated subsidiaries will automatically be covered by the regulation, regardless of their size. Smaller companies may also be covered by the Cybersecurity Act if:

1. the operator is the sole provider of a service in Sweden that is essential for maintaining critical societal or economic activities,
2. a disruption of the service provided by the operator could have a significant impact on the protection of human life and health, public safety or public health, or could entail significant systemic risks,
3. the operator is of particular importance at national or regional level for a particular sector or type of service or for other sectors that depend on the operator, or
4. the operator provides trusted services.

To fall within the scope of the Cybersecurity Act, the company shall be established in Sweden.

Non-compliance may result in significant administrative fees

Non-compliance with the obligations of the Act may result in sanctions, including administrative fines issued by the supervisory authority. The administrative fine shall be set at a minimum of SEK 5,000 and at most:

1. the higher of 2 percent of the total global annual turnover for the preceding financial year or an amount in kronor equivalent to EUR 10,000,000 for an individual operator classified as essential,
2. the higher of 1.4 percent of the total global annual turnover for the preceding financial year or an amount in kronor equivalent to EUR 7,000,000 for an individual operator classified as important, or
3. SEK 10,000,000 for public-sector operators.

Contact in Sweden

Linn Hammoud

Legal Counsel

T +46 76 503 81 03
linn.hammoud@roedl.com
www.roedl.se

The Nordic-Baltic IP, Privacy and Compliance team: your trusted partner

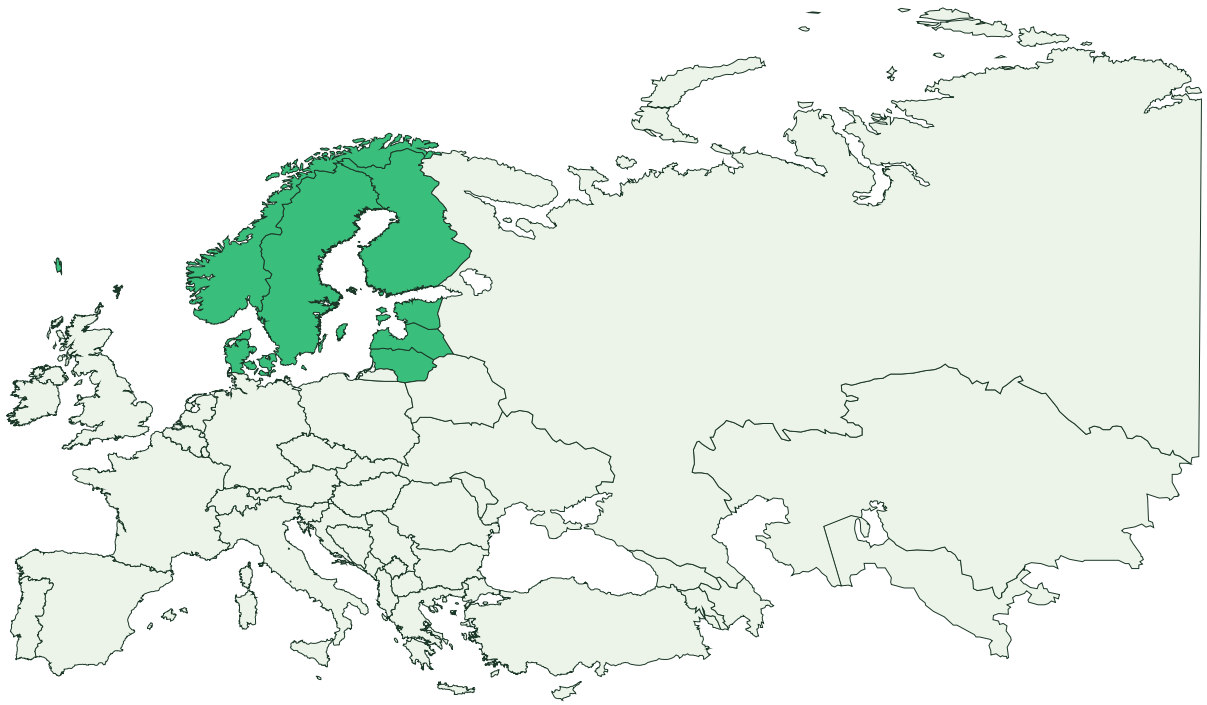
Since 1977, RÖDL has been both trusted partner and trailblazer. Across borders, we deliver solutions that make an impact – through legal advisory, tax consulting, audit and assurance, advisory sand IT, and business process outsourcing. Future-focused, across disciplines, and from a single source. With a global mindset and strong local presence. By leading the way, we make sustainable success a reality for our clients.

With currently over 117 offices in 50 countries, our clients trust more than 6.000 of our colleagues.

In the Nordic and Baltic Region, RÖDL has been present for over 30 years, supporting some of the most important investment and transaction projects.

We operate through offices in Denmark, Estonia, Finland, Latvia, Lithuania, Norway and Sweden, offering a wide range of services including legal, tax, BPO and audit consulting. We specialize in supporting both local and international clients with tailored solutions, particularly in cross-border business and compliance.

We pave the way. Worldwide.



Our IP, Privacy and Compliance services

INTELLECTUAL PROPERTY

- IP protection strategy development
- IP rights securing by agreements and registrations
- Trademark and design searches, monitoring and
- registrations
- IP protection on customs
- SaaS and licensing agreements
- IP in employment, management, service, cooperation and shareholder relations
- IP due diligence in transactions
- Enforcement and defense of IP rights

PROTECTION OF INFORMATION

- Confidential information handling policies
- Information security policies
- NDA, other trade secret related agreements
- Non-circumvention agreements
- Know-how securing and transfer agreements

DATA PROTECTION

- Privacy policies (GDPR-compliant)
- Cookie policies and consent tools
- Data Protection Impact Assessments (DPIA)
- Data breach notification procedures
- Data processing agreements (DPA)
- Cross-border data transfers (SCCs, adequacy)
- Employee data handling and internal policies

REGULATORY COMPLIANCE

Cybersecurity and Resilience

- DORA: ICT risk, incident reporting, third-party oversight
- NIS2: essential entities, supply chain risk, notification duties
- ISO 27001 alignment and audits

AI and Data Regulation

- AI Act: risk classification, transparency, documentation
- Data Act: B2B/B2G sharing, cloud portability, fair contracts
- Data Governance Act: trusted intermediaries
- Digital Services Act: platform accountability

AML and Sanctions Regime

- AML procedures – audit, policies, manuals
- Sanction regimes and export controls
- Sanction compliance clauses and declarations
- Consultations regarding AML and sanctions

- Cooperation partner screening in publicly available databases
- UBO disclosure and verification

Nordic-Baltic Focus

- Local implementation tracking
- Sector-specific compliance strategies
- Cross-border regulatory harmonization

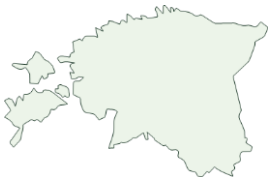
Your IP, Privacy and Compliance contacts in the Nordic-Baltic Region:

Denmark

Navina Jegarubanathan
Attorney-at-law
M +45 6052 4304
navina.jegarubanathan@lead-roedl.dk

Estonia

Alice Salumets
Partner, Attorney-at-law
M +372 606 8650
alice.salumets@roedl.com

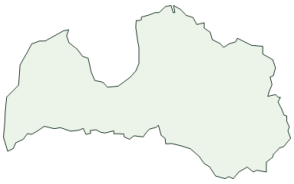


Finland

Nora Haapala
Associate Partner, Attorney-at-law
M +358 40 665 5011
nora.haapala@roedl.com

Latvia

Staņislavs Sviderskis
Manager, Assistant Attorney
M +371 2910 8644
stanislavs.sviderskis@roedl.com



Lithuania

Laima Nevarauskaitė
Senior Associate, Assistant Attorney
M +370 6023 0361
laima.nevarauskaite@roedl.com

Norway

Anniken Ramse
Partner, Attorney-at-law
M +47 917 11 517
ara@seland-roedl.no

Sweden

Linn Hammoud
Legal Counsel
M +46 76 503 81 03
linn.hammoud@roedl.com

Imprint

Publisher:
Rödl Lithuania
Aludarių Str. 1, LT-01113, Lithuania
T +370 5 2123 590
www.roedl.lt

Responsible for the content:

Navina Jegarubanathan
navina.jegarubanathan@lead-roedl.dk

Nora Haapala
nora.haapala@roedl.com

Inese Kalnāja
inese.kalnaja@roedl.com

Laima Nevarauskaitė
laima.nevarauskaite@roedl.com

Anniken Ramse
ara@seland-roedl.no

Linn Hammoud
linn.hammoud@roedl.com

Layout/typesetting:
Lina Pradkelienė
lina.pradkeliene@roedl.com