*38th International Electric Vehicle Symposium and Exhibition (EVS38) Göteborg, Sweden, June 15-18, 2025*

# The Data Regulation Puzzle of EV Charging

Jeanette Andersson[1], Emma Pakki

[1]*Jeanette Andersson (corresponding author) Swedish National Road and Transport Research Institute (VTI) Regnbågsgatan 1, 417 55 Göteborg, jeanette.andersson@vti.se*

## Executive summary

The EV charging infrastructure is crucial for EU's green transformation goals. This paper examines the EU regulatory initiatives Data Act, AI Act, and NIS2 Directive in connection with EV charging. EV charging is a delicate balance act of promoting sustainability and convenience while protecting privacy, security and safety concerns. Findings emphasize the need for legal clarity, research, and regulatory development.

*Keywords: AI – Artificial intelligence for EVs, Cybersecurity, Smart charging, V2H & V2G, Smart grid integration and grid management*

## 1 Abstract

Electromobility offers great potential for the green transformation and decarbonization of the transport sector. The rollout of EV charging is in this context considered critical for the EU energy transition [1]. To meet the objectives of the EU Green Deal and Sustainable and Smart Mobility Strategy for 2030 the European Commission has promoted cooperation between the energy and digital sectors. [2], [3]. In this cooperation data sharing and artificial intelligence play a crucial role. Provision of digital technologies can facilitate system optimization, support integration of the energy system and ease optimization of the use of grid capacity. AI could be used for demand prediction and charging grid integration [4]. However, digitalization and data sharing bring challenges and risks, exposing the users and stakeholders of EV charging and the energy system to cyberattacks and other data-related hazards. To promote data sharing while protecting these, the EU has taken regulatory action to develop legal frameworks. It has been emphasized that "data sharing frameworks are key in the realization of smart charging initiatives" [5]. However, it has also been pointed out that "the data sharing aspect of EV smart charging remains largely unaddressed and unexplored" [5]. This warrants further studies to better understand the regulatory challenges and how such frameworks should be construed and interpreted to support the rollout of efficient and secure EV charging.

The aim of this paper is to identify and map the key EU regulatory developments as well as to contribute to the regulatory discussions on the data, AI and cybersecurity regulation challenges applicable to EV charging. This includes analyzing these initiatives to clarify their legal effects and impact on EV charging. A combination of methods is employed including a literature review regarding EV charging and the regulatory initiatives on both Swedish and EU level. Legal analytical method is used to interpret these initiatives. Interviews, dialogues and workshops have also been performed. The focus is on the Data act, AI act, and the NIS2 directive [6], [7], [8]. Where relevant, other regulatory initiatives and standards have been discussed.

## 2 Data sharing and the Data Act

One vital piece of the data regulation puzzle of EV charging is the Data Act, being a cross-sector regulation with the aim of promoting data. The Data Act entered into force on 11 January 2024, and it will become applicable on 12 September 2025 [9]. It is a key pillar of the European strategy for data [10] and complements the Data Governance Act which became applicable in September 2023 [11]. Whereas The Data Governance Act regulates the structure and processes providing a framework to enhance trust in voluntary data sharing, the Data Act provides regulation on the access to and use of data. Both Acts are cross-sectorial.

The Data Act is structured in 11 chapters including provisions on different relationships and topics. Inter alia, there are chapters addressing business-to-business and business-to-consumer data sharing in the context of IoT (chapter II), business-to-business data sharing (chapter III), and business-to-government data sharing (chapter V). In addition, there is a chapter on unfair contractual terms (chapter IV) protecting all businesses, in particular SMEs, against such terms imposed on them. Other issues addressed include switching between data processing services (chapter VI), interoperability (chapter VIII), unlawful third country government access to data (chapter VII) and enforcement (chapter IX). The Data Act applies to manufacturers, users, data holders, data recipients, public sector bodies, providers of data processing services, participants in data spaces and vendors of applications using smart contracts [12].

A core implication of the Data Act is that it fundamentally changes how numerous vehicle manufacturers manage data generated by the vehicles. It requires them to open their data ecosystems to third parties in accordance with fair and transparent conditions. Thus, vehicle owners are empowered to access the data generated by their vehicle use and reap the value of it [13]. As such, the Data Act implies a shift of data control to drivers, fostering a "driver-centric mobility data ecosystem" [14]. In the EV charging context the owners could for instance benefit from charging optimization making it cheaper and more efficient through rewards programs, smart scheduling and home integration. Also, the Data Act introduces rules for situations where a company has a legal obligation to make data available to another company on fair, reasonable and non-discriminatory terms for reasonable compensation. The interpretation of reasonable has been much debated [15], but the Data Act mandates the European Commission to adopt guidelines on the calculation of such compensation. In addition, the Act is to be complemented with delegated and implementing acts [6].

Other provisions with high relevance in an EV charging context aim to ensure interoperability between data processing services through harmonized standards and open operability specifications. Such standards governing EVs communication and charging infrastructure are crucial. One important example is the international ISO 15118 standard, which defines the communication protocol between electric vehicles and charging stations. Also, the Data Act includes essential requirements to allow data to flow within and between so-called data spaces, making it available for access and reuse to the participants [16]. In this context, the implementing EU-Regulation as regards specifications and procedures relating to the availability and accessibility of data on alternative fuels infrastructure should be briefly mentioned [17]. The Regulation further advances the goals set out in the Alternative Fuels Infrastructure Regulation (AFIR) [18]. It includes detailed rules and data specifications to ensure greater transparency, interoperability, and accessibility of recharging and refueling infrastructure data for alternative fuel vehicles. The Regulation complements a broader package of four legislative Acts on data and standards [19] with the following objectives: to ensure minimum infrastructure to support the required uptake of alternative fuel vehicles across all transport modes and in all EU Member States to meet the EU's climate objectives; to ensure full interoperability of the infrastructure; and to ensure comprehensive user information and adequate payment options at alternative fuels infrastructure [20].

In addition to the above, it should be mentioned that the European Commission, in March 2025, set out concrete measures to support the automotive sector in an Industrial Action Plan [21]. Among others, complementary and adequate measures to facilitate bi-directional and smart charging as well as access to vehicle data are set out. Also, a Guidance on in-vehicle data will be published at the start of application of the Data Act and, if needed, a legislative proposal on access to such data will be considered. Furthermore, reference is made to the possible establishment of a European Automotive Data Platform, considering also cybersecurity concerns for remote access to data [22].

To sum up, the Data Act is a key pillar of the European strategy for data and highly relevant for EV charging. However, it is only one piece of many regulatory data sharing initiatives. The mapping shows that the data regulation puzzle of EV charging is construed by a complex mix of cross-sector and sector-specific regulations and directives as well as standards and protocols, see figure 1.

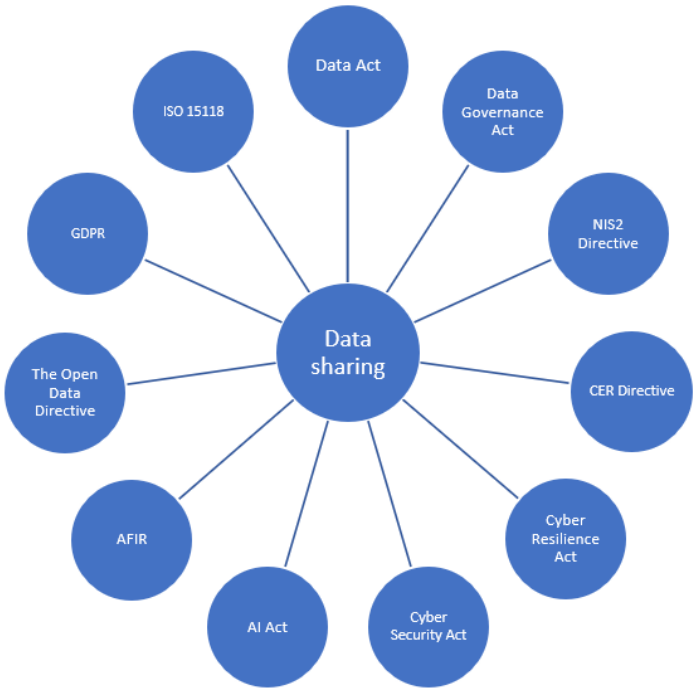


Figure 1: A selection of different data regulations and standards that may affect EV charging.

# 3 Artificial intelligence and the AI Act

AI is one of the most frequently used digital technologies in electricity systems [23]. AI regulation in Europe is, however, a new concept and the balancing between innovation and regulating AI is said to be challenging [24]. On August 1, 2024, the AI Act came into force. Most parts of the AI Act will be applicable 24 months thereafter and some parts after 36 months. However, the parts concerning prohibitions became applicable 6 months after the enforcement, thus on 2 February 2025. The purpose of the AI Act is to ensure that the AI-systems in EU are safe and facilitate innovation and investment concerning AI [25]. The AI Act aims to lay down regulation concerning the following areas:

- Placing and using of AI-systems
- Prohibitions
- High-risk AI systems
- Transparency
- Placing of general-purpose AI models
- Market monitoring, market surveillance, governance and enforcement
- Measures to support innovation

Risks in the AI Act are divided into four different levels [26]:

- *Unacceptable risk*, which is prohibited in accordance with article 5 AI Act. Such risks include, for example, manipulative AI and social scoring.

- *High risk* in accordance with article 6 AI Act, which means AI that may affect safety or fundamental rights. The risk may stem from the way a system is designed or how it is used [27].
- *Limited risk* applies to certain AI systems mentioned in article 50 AI Act. The systems included are those intended to interact with people or generate information. The systems are not likely to cause significant harm or affect fundamental rights and are thus subject to lower requirements and only triggering requirements concerning transparency [28].
- *Minimal risk or no risk.* The AI Act does not include rules för AI with minimal or nor risk, such as, for example, AI-enabled video games or spam filters [29].

For the purpose of this article high-risk AI systems will be discussed more into depth. Both due to the extensive requirements that are imposed on these systems but also since motor vehicles may fall within the scope of the AI Act. Article 6 AI Act defines which AI systems that should be considered as high-risk AI systems. Motor vehicles may fall within the scope of high-risk AI systems [30]. However, the AI Act does not apply directly to auditing of the vehicle system since sectorial regulations such as the Type-Approval Framework Regulation (TAFR) [31]. AI-systems linked to charging could be defined as a high-risk AI-system if it is used as a safety component in critical infrastructure in accordance with article 6.2 and annex III.[32]. However, this is only likely under certain circumstances, for example, if a malfunctioning affects critical infrastructure [33].

When a system is considered to be a high-risk AI system, and when it is not excluded from application of the AI Act due to sectorial regulation, such system has to comply with several requirements as listed below.

- Risk management system (article 9)
- Data and data governance (article 10)
- Technical documentation (article 11)
- Record keeping (article 12)
- Transparency and provision of information to deployers (article 13)
- Human oversight (article 14)
- Accuracy, robustness and cybersecurity (article 15)

Even though the AI Act now is in place, several questions of how it should be interpreted remain. One challenge is that the sectorial legislation will undergo changes to be adapted to the requirements of the AI Act. It is not clear, as of yet, if these revised obligations will fully correspond with the requirements of the AI Act. The actors in the supply chain therefore risk being affected by different rules in different legislations [34]. One major legal challenge concerning the AI Act is article 14, dealing with how human oversight should be interpreted [7]. There are uncertainties about how much oversight is necessary, what constitutes sufficient human control, and who will be held liable if something goes wrong despite the presence of human oversight. Further issues concerning AI liability is not regulated in the AI Act. There have been EU-initiatives concerning an AI liability Act but this process has been withdrawn. Currently, liability is therefore going to be addressed by national regulations [35], thus creating a regime where liability may differ between different jurisdictions. The withdrawal decision is new and is yet to be evaluated. However, the authors of this paper hold that this may result in legal uncertainty and, thus, a barrier for the use of AI in full scale in EV charging scenarios.

# 4 Cybersecurity and the NIS2 Directive

Last year, the global costs of cyberattacks were estimated to $9,5 trillion. Also, it was held that cyberattacks occur 2 200 times daily [36]. Even though the exact numbers are difficult to determine, partly due to a large number of unreported cases [37], it can be said that the numbers are worrying and that they probably will increase [38]. EV charging stakeholders are involved in issues concerning connection to the grid and are often accountable for data such as payment information and user identities. This complex interconnection is affected by an range of cyberthreats including risk of disruption to the power grid as well as data breaches [39]. To address these issues, the EU has developed cybersecurity regulation. For the purpose of EV-charging the CER Directive (CER) [40], Cyber resilience act (CRA) [41], Cybersecurity act (CSA) [42] and the NIS2 Directive (NIS2) [8] ought to be mentioned. The purpose of CER is to enhance the resilience and capacity of

critical operators who provide essential services within the internal market. The purpose of CRA is to increase security and resilience to cyberattacks against products with digital elements. CSA is establishing a common framework cyber security certification and is also giving mandate to EU Agency for Network and Information Security (ENISA). The purpose of NIS2 is to strengthen cybersecurity for essential services through establishing a high level of security for network and information systems [8]. Many actors will fall within the scope of NIS2. Further, the regulation came into effect in October 2024 and is currently being implemented into the national laws of the EU members. For the purpose of this paper NIS2 will be described more in depth hereinunder.

NIS2 is replacing the NIS Directive [43], imposing clearer requirements and including more entities in its scope. NIS2 applies, for example, to entities acting within the sectors of energy, manufacturing and digital infrastructure. As a result, manufacturers of vehicles, charging point operators (CPO) and charge point management systems (CPMS) could be included in the scope [8], [44], [45]. However, the underlying principle is that individual operators must have 50 employees or an annual turnover of €10 million to be included in the scope. Also, smaller operators may according to NIS2 be included in the scope if certain exemptions apply. The exemptions include, for example, entities which are critical because of their specific importance at national or regional level and certain public administration entities [46]. However, other exemptions might be applied, and it is up to the member state to identify the exemptions [47].

NIS2, in comparison with for example the AI Act, does not include prohibitions. Instead, it imposes various security requirements on operators. The stakeholders included in the scope of NIS2 must, for instance,

- register their organization (Article 3.4)
- implement cyber security risk management measures (Article 21.1-21.3)
- report significant incidents (Article 23)
- educate management and offer employees training in risk management measures (Article 20.2)
- if the organization is involved in cross-border activities without an establishment in the EEA, it must appoint a representative in one of the countries where services are offered (Article 26).

The cyber security risk management measures are imposing high demand on entities. Entities should take appropriate and proportionate technical, operational and organizational measures to manage risks. The measures shall be based on an all-hazards approach aiming at protecting network and information systems and its physical environment [48]. There are several risk management measures, for example, entities must have strategies for risk analysis and information security, incident handling, business continuity, supply chain security and security concerning acquisitions [49].

The supply chain security requirement has been widely debated since it in fact imposes cyber security requirements on suppliers who are not included in the scope of NIS2, for example suppliers outside EU. The article make reference to “direct suppliers”. In the Swedish Government Official Report concerning NIS2 it is concluded that it implies that the entities only are responsible for the first step in the supply chain [50]. The detailed interpretation of the supply chain security requirement is stated to be outlined in national regulations, according to the Swedish Government Official Report. However, one of the likely main effects of this requirement is that entities now need to update their contracts to include provisions concerning NIS2 [51]. In many contractual relationships it is not possible to have control over the wording in a contract. This could, for example, be the case when the supplier is a holder of open-source software which often make use of non-negotiable license agreements [52]. Another possibility is that suppliers get certified under the harmonized certification system “EU Certification Scheme” which has been introduced in line with the new regulation CSA [53]. However, the certification schemes are under development and the first certification scheme is fully applicable from February 2025 [54]. There is also valuable guidance in ENISA's report on "Good Practices for Supply Chain Cybersecurity" recommending different ISO-standards and the NIST cyber security frameworks [55]. The report is also, inter alia, stating that entities should take the following into account:

- Risk factors and results of coordinated risk assessments made by EU

- Available country specific information
- Restrictions or exclusions stemming from a relevant national authority
- Known threats or incidents
- The quality of the relevant supplier such as quality of security measures, level of transparency and the legal framework etc. [56].

Further, it should be mentioned that if an entity included within the scope of NIS2 does not fulfill the provisions in NIS2 the competent authorities of the member states shall use effective, proportionate and dissuasive measures. The authorities shall inter alia have powers to decide about administrative fines for essential entities up to the highest amount of EUR 10 000 0000 or 2% of the worldwide turnover in the preceding financial year. For important entities the fines are slightly lower [57]. Another tangible sanction is the possibility for authorities to force an entity to publicly disclose violations of NIS2 [58].

# 5 Conclusion

The main conclusion is that data regulation addressing EV charging is a delicate balance act of promoting sustainability and convenience while protecting privacy, security and safety concerns. The amount and complexity of the regulations and directives require a high level of legal knowledge to understand and comply with the requirements. Such demands on stakeholders entail high transaction costs. Also, the legal uncertainty of the content, interpretation and implications of the regulations is a barrier for an efficient and speedy rollout of EV charging infrastructure. It should be highlighted that the importance of future case law as well as legal research and doctrine to develop a thorough understanding of the data regulation ecosystem and its legal implications cannot be underestimated. Compliance may in some cases be facilitated through certification, standards and frameworks. The regulatory puzzle is still incomplete and under construction. There are many missing pieces to form an adequate picture.

# Acknowledgements

This paper is based on work in the ongoing project DataREgulation And electroMobility (DREAM), funded by the Swedish Electromobility Center, coordinated by the Swedish National Road and Transport Research Institute (VTI), Ref. No 2021-0017. The authors would like to acknowledge and express their gratitude and appreciation to the project team members Daniel Rudmark and Erik Nyberg who have provided valuable input on the data sharing aspects as well as the reference group members from Volvo Cars, Scania and Zeekr for their support and insightful discussions during the project.

# References

[1] Ennis, Sean & Colangelo, Giuseppe. *Energy data sharing and the case of EV smart charging*. (2022).
[2] European Commission. *European Commission Digital Strategy* C (2018) 7118 final, 21 November 2018.
[3] European Commission. *Roadmap to the Action Plan on the Digitalisation of the Energy Sector*, (2021).
[4] Farnsworth, Elaine. *AI Putting a Charge into EV Charging Stations. Discover the future of EV (electric vehicle) charging with AI-driven predictive analytics*. (2024). https://www.spiceworks.com/tech/artificial-intelligence/guest-article/ai-putting-a-charge-into-ev-charging-stations/ accessed 31 October 2024.
[5] Ennis, Sean & Colangelo, Giuseppe. *Energy data sharing and the case of EV smart charging*. (2022).
[6] The European Parliament. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).
[7] The European Parliament. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).
[8] The European Parliament. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).
[9] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). The Data Act was published in the Official Journal of the European Union on 22 December 2024.
[10] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. A European strategy for data. COM/2020/66 final.
[11] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

[12] Art. 1, sec. 3. Data Act.
[13] Lundqvist, Björn. *Regulating Access and Transfer of Data. Cambridge University Press*. (2023).
[14] Katta, Sahas. The EU Data Act: A catalyst for change. (2025).
[15] Fritz, Gernot & Cuvan, Tina F. & Ehlen, Theresa & Werkmeister, Christoph & Dannhausen, Estella. *A Game-Changer in Data Regulation: The EU Data Act unpacked.* (2024).
[16] See more about Common European Data Spaces on https://digital-strategy.ec.europa.eu/en/policies/data-spaces.
[17] Commission Implementing Regulation (EU) 2025/655 of 2 April 2025 laying down rules for the application of Regulation (EU) 2023/1804 of the European Parliament and of the Council as regards specifications and procedures relating to the availability and accessibility of data on alternative fuels infrastructure, C/2025/1917.
[18] Regulation (EU) 2023/1804 of the European Parliament and of the Council of 13 September 2023 on the deployment of alternative fuels infrastructure, and repealing Directive /94/EU.
[19]https://transport.ec.europa.eu/news-events/news/commission-enhances-interoperability-and-transparency-alternative-fuels-infrastructure-data-2025-04-11_en.
[20]https://transport.ec.europa.eu/transport-themes/clean-transport/alternative-fuels-sustainable-mobility-europe/alternative-fuels-infrastructure_en.
[21] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. Industrial Action Plan for the European automotive sector. COM/2025/95 final.
[22] Action Plan for the European automotive sector, pp. 5-6.
[23] Fabian Heymann, Tatjana Milojevic, Andrei Covatariu, Piyush Verma, *Digitalization in decarbonizing electricity systems – Phenomena, regional aspects, stakeholders, use cases, challenges and policy options*, Energy Reports, Volume 262, Part B, (2023).
[24] F. Heymann, K. Parginos, R.J. Bessa, M. Galus, *Operating AI systems in the electricity sector under European's AI Act – Insights on compliance costs, profitability frontiers and extraterritorial effects*, Energy Reports, Volume 10, (2023).
[25] Recital (1) AI Act.
[26] https://artificialintelligenceact.eu/high-level-summary/.
[27] Recital (93) AI Act.
[28] See also https://www.lexology.com/library/detail.aspx?g=68bb1057-cf61-4d48-bc50-f7e010581cba.
[29] https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.
[30] See article 6 AI-act and https://www.europarl.europa.eu/pdfs/news/expert/2023/6/story/20230601STO93804/20230601STO93804_sv.pdf.
[31] See article 2.2 AI act and https://www.taylorwessing.com/en/interface/2024/ai-act-sector-focus/eu-ai-act-and-the-automotive-industry.
[32] See article 6.2 listing that systems referred to in Annex III in the AI act also can be defined as a high-risk AI-system.
[33] Operating AI systems in the electricity sector under European's AI Act – Insights on compliance costs, profitability frontiers and extraterritorial effects, Energy Reports, Volume 10, (2023).
[34] https://www.holisticai.com/blog/driving-innovation-navigating-eu-ai-acts-impact-on-autonomous-vehicles.
[35] https://iapp.org/news/a/european-commission-withdraws-ai-liability-directive-from-consideration.
[36] https://keepnetlabs.com/blog/171-cyber-security-statistics-2024-s-updated-trends-and-data.
[37] See inter alia MSB – Myndigheten för samhällsskydd och beredskap. Verktyg för ökad motståndskraft och stärkt civilt försvar.
[38] See inter alia https://www.dagensinfrastruktur.se/2024/10/29/cyberattacker-okar-med-165-procent-i-sverige-storsta-okningen-i-europa/.
[39] https://www.ampeco.com/blog/the-cpos-guide-to-the-nis2-directive/.
[40] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.
[41] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU).
[42] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
[43] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
[44] Kadiri, Ivelina. *The CPO's guide to the NIS2 directive.* (2024). https://www.ampeco.com/blog/the-cpos-guide-to-the-nis2-directive/.
[45] Statens Offentliga Utredningar, *Nya regler om cybersäkerhet* (SOU 2024:18).
[46] See article 2.2 e-f.
[47] See article 2.2 b-f and article 3.1 e. See also SOU 2024:18 s. 144.
[48] Article 21.1 NIS 2.
[49] SOU 2024:18 p.41-42, Art 21 NIS2.
[50] SOU 2024:18 p. 195.
[51] For an example, see https://www.shoosmiths.com/insights/articles/nis2-is-here-what-energy-utility-providers-need-know-about-europes-new-cybersecurity-regime.
[52] M.Papaphilippou, K. Moulinos, M. Theocharidou, Good practices for supply chain cybersecurity, https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity (2023), p.5.
[53] https://certification.enisa.europa.eu/index_en and M. Papaphilippou, K. Moulinos, M. Theocharidou, Good practices for supply chain cybersecurity, https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity. (2023) p. 12.
[54] Cybersecurity Certification Scheme on Common Criteria (EUCC)
Seehttps://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en and https://www.fmv.se/verksamhet/ovrig-verksamhet/nationella-myndigheten-for-cybersakerhetscertifiering/det-europeiska-ramverket-for-cybersakerhetscertifiering/common-criteria/.
[55] https://certification.enisa.europa.eu/index_en. and M. Papaphilippou, K. Moulinos, M. Theocharidou, Good practices for supply chain cybersecurity, https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity (2023) p. 38.
[56] https://certification.enisa.europa.eu/index_en. and M. Papaphilippou, K. Moulinos, M. Theocharidou, Good practices for supply chain cybersecurity, https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity (2023) p. 22.

[57] Article 34 NIS2.
[58] Article 23.4 g.

## Presenter Biography

**Emma Pakki** holds a law degree from Umea University and a master's degree in Maritime and Transport Law from the University of Southampton. She has professional experience in law firms, courts, and the municipality before taking on her current role as a research assistant at VTI. Emma is currently involved in a project on data regulation and mobility called DREAM. Additionally, she is working on a project related to digital location guidance for underground cables. Both projects focus on data regulation, AI regulation, and cybersecurity. Furthermore, she participates in various initiatives related to autonomous ships and vehicles.

**Jeanette Andersson** is a Doctor of Laws and senior researcher at the Swedish National Road and Transport Research Institute (VTI). She has a professional background from academia working as a lecturer at the department of law at Gothenburg University and Örebro University and from working as a legal counsel and in court. In 2018 she obtained her Doctor of Law degree on a thesis about ship management contracts. She is currently a project leader of a project on data regulation and electromobility. Furthermore, she is also involved in several research projects on remote operations and connected and automated driving.