impl | Implementeringsrådet

2025-08-25
Komm2025/ 00057

The Swedish Implementation Council
KN 2024:04

Ministry of Defence, Cyber and Hybrid Affairs Unit (ECH)

Ministry of Justice
Constitutional Unit (Ju L6)

Copy sent to: KN, NIM

Basis for Sweden's position for the upcoming EU negotiations – proposal for the digital package

The Swedish Implementation Council's contribution to the Swedish position is presented in its entirety in section 5. The Council's proposals in summary are:

- Clarify overlaps, contradictions and terminology between EU legal acts in the fields of cybersecurity, digitalisation and artificial intelligence.
- Introduce more uniform and consistent criteria and requirements for reporting incidents.
- Let the CSA certification be valid for overlapping requirements.
- Ensure that cybersecurity regulations do not impede data transfer or thwart global data flows.

1. Task of the Swedish Implementation Council

The Swedish Implementation Council is tasked with assisting the Government in its efforts to strengthen the competitiveness of Swedish companies by avoiding implementation above the minimum level and counteracting unjustified regulatory burdens, as well as reducing administrative costs and other compliance costs in connection with the implementation of EU regulations in Swedish law. The Implementation Council's work must be based on a company perspective.

STATENS OFFENTLIGA UTREDNINGAR

The Implementation Council is to submit documentation and recommendations to the Government, partly as a contribution to Swedish positions in negotiations and partly on how EU legal acts can be implemented in Swedish law in a way that is not more far-reaching from a business perspective than what the legal acts require.

The Implementation Council's work is based on problem descriptions that have been communicated to the Council, mainly from industry organisations and their member companies. During the work on the documentation, contacts are also made with others who are familiar with the respective subject area, such as government agencies. In the light of the information and knowledge gathered and in the context of the overall objective of the act in question, the Council makes a balanced and independent assessment of how the business perspective can be effectively addressed in each case.

In preparing this opinion, the Council has mainly used documentation received through conversations with experts/business experts from: Svenskt Näringsliv, Teknikföretagen, SOFF, Almega, TechSverige, Svensk Bankförening, Visita, Transportföretagen, Livsmedelsföretagen, Svensk Handel och Ikem. In addition, the Implementation Council has taken note of written proposals and compilations from Digital Europe and Orgalim.

Relevant EU legal acts

The European Commission has announced that a proposal called the digital package (omnibus) will come by the end of 2025. It is not fully known at the time of writing this opinion what will be included in the Commission's digital package. Among other things, there is information that revisions to the Cybersecurity Act (CSA) will be included. Previously, it has been discussed that the changes to the General Data Protection Regulation (GDPR) would also be included in this omnibus package. However, this has changed and is now planned to be presented separately in early 2026 (announced at the stakeholder dialogue on 15 July by DG Justice). This opinion is therefore not intended to cover the companies' whole perspectives and future submissions regarding revisions of the GDPR.

Objectives and objectives of the EU legal acts

Revisions of the Cybersecurity Act
Revisions of the CSA aim to simplify, ensure synergies between initiatives related to improving the Union's preparedness, as well as to reduce the administrative burden and streamline implementation for businesses. The aim is to streamline cybersecurity measures, strengthen cyber resilience and achieve a high common level of cybersecurity across the EU.

The revisions will mainly include: the mandate of the European Union Agency for Security (ENISA), to develop the Common Cybersecurity Certification Framework (ECCF) for increased resilience, and to address challenges related to the security of the ICT supply chain. The revisions have been initiated by ENISA in light of the rapid developments in cybersecurity, including in terms of complexity and number of attacks. There have also been several other related acts following the introduction of the CSA, which have affected ENISA's role and mission.

The introduction of CSA about six years ago (in 2019) meant, among other things, the establishment of a common certification framework for ICT products and processes, the European Cybersecurity Certification Framework (ECCF). It was introduced with the aim of, among other things, protecting industries, citizens and critical infrastructure from internal and external threats. Among other things, there is a need to improve the certification framework and clarify the roles and responsibilities of different actors throughout the process of strengthening security throughout the value chain.

The planned amendments to the GDPR aim to simplify the legislation that entered into force in 2018. It is not yet known to what extent the GDPR will be opened up for revision.

The introduction of the GDPR imposed stricter requirements on the processing of personal data with the aim of protecting the fundamental rights and freedoms of individuals, in particular their right to the protection of personal data. The regulation covers all companies that handle personal data.

Omnibus IV proposes to amend Article 30 of the GDPR (register of processing), [1]changes that the Council will not touch on in detail in this opinion.

2. Where are the proposals in the process?

The proposal for the Digital Package has been announced in the Commission's Work Programme for 2025. Revisions to the Cybersecurity Act have been out for consultation between 11 April and 20 June 2025. Amendments to the GDPR have been discussed in a meeting between the Commission and industry leaders, industry groups and civil society organisations in mid-July 2025, and a special meeting on this is planned for September.

Formal proposal from the Commission on the Digital Package is planned for Q4 2025, probably in December. There is no written proposal from the Commission yet. The information available is set out, inter alia, in the Commission's consultation document on the Cybersecurity Act.

Despite this early stage and the relatively limited documentation available on the changes in the digital package, the Implementation Council considers it important to submit an opinion. This is based on the fact that the proposal has consequences for a wide range of entrepreneurs and that the relevant industry organizations have received several views and submissions as well as alternative proposals. The opinion can form the basis for bilateral contacts with the Commission, submissions in the ongoing consultation process or other advocacy work at an early stage.

3. Responsible ministry

The Ministry of Defence is responsible for revisions of the Cybersecurity Act, while the Ministry of Justice is responsible for the GDPR, which are covered by this opinion. In the final proposal for the digital package (the omnibus), the Ministry of Finance will also be responsible for the relevant acts.

[1] At present, companies with fewer than 250 employees are not required to keep records of all personal data processing, as long as the processing does not involve special risks. The Commission proposes that this exemption should also apply to companies with up to 750 employees, provided that the processing is not of such a nature that it poses a "high risk" to the data subjects.

Problem description from a Swedish business perspective

Regulations in digitalisation, cyber security and automation have taken place with a high intensity, which has meant that the legislations as a whole are perceived as convoluted and not adapted to each other.

The majority of the industry associations mentioned are generally neutral or positive to proposed revisions of the Cybersecurity Act. Among other things, it is mentioned that it is welcome that ENISA will be given an expanded mandate and responsibility.

With regard to the GDPR, there are concerns, among other things, about whether the entire regulation will be opened up for revision. It is considered that necessary changes and corrections can be made without opening up the entire regulation. The business community wants to continue to retain the basic principles of GDPR, but there is a need for regulatory simplification when it comes to administrative burdens where the requirements are considered disproportionate and too burdensome.

The main areas of concern identified in relation to EU legal acts are summarised below.

Overlapping EU legal acts in the digital area entail increased reporting requirements

The rapid development and regulation of digitalisation, cybersecurity and artificial intelligence has given rise to overlaps between EU legal acts, which has led to, among other things, increased reporting requirements for companies and, in some cases, double reporting of similar information to different authorities. The criteria for reporting incidents also differ (thresholds, timelines and reporting templates) at present, and companies are expected to report incidents according to, among other things, GDPR, Network and Information Systems Directive 2 (NIS2), The Digital Operational Resilience Act (DORA) and the Cyber Resilience Regulation (CRA). There are also differences in the definition of "risk" between NIS2, GDPR and the Cyber Resilience Act.

This makes it difficult for companies to live up to the requirements of the legislation as it is challenging and takes time from production/core business to familiarize themselves with the regulations, the various reporting criteria and templates, and that reporting takes place in different systems. This is

especially true for smaller companies where resources and skills are more limited.

For example, the Copyright Act, the AI Regulation and GDPR are described as related and partly overlapped. The same applies to the Platform Directive, the NIS2 Directive and the AI Regulation, which in some cases can be seen as complementary[2]. There is a need to clarify the relationship between these in order to facilitate companies' regulatory compliance. The law with the highest requirements should then be the starting point for harmonisation.

In the financial sector, the example of how CRA and DORA overlap is highlighted and there is a lack of a clear hierarchy between them. They both aim to improve cybersecurity but from different perspectives, CRAs with horizontal rules for digital products while DORA includes a resilience framework specific to the financial sector.

There are more examples of overlapping legislation in the area than mentioned above[3].

Inconsistent terminology between acts, regulations and directives creates unnecessary complexity and is administratively demanding

There is a terminology confusion between most regulations in the digital area where similar or similar terms and concepts are defined differently. This leads to challenges in interpreting, understanding and complying with the regulations for companies and becomes administratively demanding.

For example, the CSA has a definition of "ICT product" and the CRA defines "product with digital elements". These are examples from horizontal legislation, in addition to which the definitions of products are found in sector-specific rules that are added. All of these laws have requirements for products to be placed on the EU market and they are applied at the same time.

---

[2] The three sets of rules aim to protect fundamental rights. The NIS2 Directive focuses on security and privacy, the Platform Directive on equal treatment and working conditions, and the AI Regulation on ensuring that AI systems do not harm health, safety or democracy. The NIS2 Directive and the AI Regulation have common points of contact on issues of security and risk management, while the Platform Directive and the AI Regulation share a focus on transparency and protection of fundamental rights.

[3] Business Europe paper – simplification of the digital rulebook (17 juli 2025).

Another example is the inconsistent definitions of "material change" in the AI Regulation, CRA and Machinery Regulation (MR). There are also several definitions of "risk" between, among others, NIS2, CRA, the AI Regulation and the General Product Safety Regulation (GPSR).

The parallel existence of voluntary certification, third-party conformity assessments and self-monitoring creates confusion

The CSA currently operates in isolation from recently enacted cyber legislation, including the NIS2 Directive and the CRA. Businesses, especially the smaller ones, face uncertainty about how voluntary CSA certification schemes interact with new cybersecurity and risk management requirements under the CRA and NIS2. The parallel existence of voluntary certification under the CSA, third-party conformity assessments, and self-monitoring creates confusion. Furthermore, it is pointed out by most industry representatives/companies that it is important to continue to have the CSA certification primarily as an elective based on the fact that it allows lower thresholds for market access, entails lower costs and promotes innovation.

There are also concerns that the CRA, which does not currently require mandatory certification for any product category, may be amended in future delegated acts and introduced as an obligation. Currently, the CRA complies with the New Legislative Framework (NLF), which allows for the use of proportionate assessments of risk and cybersecurity aspects, including self-monitoring for low-risk products.

GDPR can complicate information transfer and limits international data transfer

Article 10 of the GDPR (processing of personal data related to criminal convictions and offences) currently makes it difficult to share information between companies and other organisations when they are exposed to, for example, cyber security threats. The industry expresses that it is primarily the Swedish interpretation of the term "personal data relating to convictions in criminal cases and offences involving offences or related security measures" that makes it more difficult. Most other EU countries have adopted a different interpretation that does not prevent information sharing in the same way.

There are also concerns that GDPR restricts data transfer globally (to third countries) and thus the ability to use and develop, for example, cloud services. Swedish and Finnish companies are among the leaders in using cloud services and it is described as an important part of developing the technology industry in the future. The importance of global cloud services and other digital infrastructure is described in the Government's strategy for cybersecurity Sweden in a digital world (December 2024).

Contradictions between the GDPR and the Data act, among other things, make it difficult and can inhibit the innovative power of companies

The industry also expresses that there are contradictions between the so-called Data act[4] requirement to make large amounts of data (including personal data) available and the GDPR's preventive prohibition against the disclosure of personal data. Although it states that the GDPR takes precedence in the event of a conflict between the two regulations, the complex interplay between the provisions is described as creating significant uncertainties for businesses on a technical and contractual level. Companies' innovation and competitiveness can be hampered when they need to devote time and energy to understanding and clarifying contradictions in legislation. The problem is pointed out to be particularly clear in the case of personal and non personal data (data that contains both personal data and other data).

Concerns that revisions in the GDPR will entail additional complexity and administration, while the legislation today is perceived as difficult to interpret

The majority of companies, especially smaller ones, still find it difficult to interpret the GDPR and understand whether or not they are compliant. These challenges are reflected, among other things, in follow-ups of the compliance rate of GDPR among Swedish companies, which show that about 37% of small companies meet the requirements and about 48% of the larger

[4] 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 (the Data Act)

companies (where the majority have a so-called Data Protection Officer).[5] It may indicate a need for further guidance and advice.

4. The Swedish Implementation Council's Analysis

Industries and companies concerned

The digital package and revisions of CSA and GDPR are expected to have a broad impact in the industry and include both large and small Swedish companies. The exact number of companies that will be affected by the revisions has been difficult to estimate, as there is limited information available on how many people process personal data and/or are affected by the amendments to the Cybersecurity Act.

Micro, small and medium-sized enterprises will be particularly affected due to their limited resources and capacity to familiarise themselves with and adapt in the light of new legislation. However, the larger companies are also affected as they have a more comprehensive system structure and in many cases operate in a global market with national differences in legislation.

Consequences for Swedish companies

Administrative and other performance costs

Inconsistent terminology between acts, regulations and directives, among other things, creates unnecessary complexity and it takes time for companies to penetrate the legislation and know whether they have really understood it correctly.

The parallel existence of voluntary certification (CSA), third-party conformity assessments, and self-checks creates confusion and administration for companies. It also entails uncertainty for companies as to whether they comply with the requirements and is also administratively burdensome.

There are concerns that a total renegotiation of the GDPR would incur costs instead of reducing the administrative burden. This is because, among other things, it becomes difficult to orient oneself and understand how companies

[5] According to surveys from the Swedish Entrepreneurship Forum and the Swedish Authority for Privacy Protection, IMY.

should adapt in practice to comply with the legislation, especially for the smaller companies.

As there is not yet a final proposal from the Commission on the digital package, it is difficult for companies to estimate the extent of the costs that the proposals will entail. However, examples of costs that could arise for companies in connection with the implementation of the digital package are:

- Costs for consultancy and/or legal costs for interpreting rules and how the company will adapt for regulatory compliance.
- Administrative costs in the form of, for example, loading, contacts with responsible authorities, reporting to supervisory authorities, development of new policies and more when changes occur.
- Administrative costs for overlapping/duplicating reporting requirements and familiarising themselves with the different reporting structures.
- Costs for any purchase of new/updated system support.

There are also parts of industries where business opportunities are created as a result of the regulatory changes, such as IT consultants and, for example, advisory consulting services within GDPR.

Other consequences and impact on the competitiveness of Swedish industry

If the revised regulations within the digital package become too extensive and complicated, there is a risk that companies will refrain from starting and scaling up business because the regulatory burden becomes a threshold.

Unclear and burdensome rules in the GDPR can cause companies (for fear of making mistakes, due to uncertainties about what is allowed or not allowed, or because of the high administrative costs that follow), to refrain from developing new digital products and services, especially those supported by AI.

Unclear and burdensome rules in the GDPR can cause companies, due to uncertainties about what is allowed or not allowed, or because of the high administrative costs that follow, to refrain from developing and developing new, efficient and innovative products and services with the help of AI. Regulations in the GDPR and the AI Regulation can lead to investments in

AI and technological development not taking place in Europe, a trend that has already been seen in, for example, the pharmaceutical industry. Access to large and qualitative data sets is central for companies to be part of this development.

There is also a risk that the willingness to invest will decrease in Swedish companies if, for example, copyright and the protection of algorithms and other information worthy of protection diminish as a consequence of demands for increased transparency in the regulations.

5. The Implementation Council's basis for Sweden's position on advocacy work and for upcoming EU negotiations on the digital package

Clarify and clarify overlaps, contradictions and terminology between EU legal acts in the fields of cybersecurity, digitalisation and artificial intelligence

- Use standardised terms and concepts in EU regulations and make it mandatory to cross-reference definitions when drafting new legislation. Also review and adapt existing legislation in this area.
- Terms and definitions for products, connected products and extensive change need to be given the same wording and explanation in CSA, GPSR, PLD, the Machinery Regulation, the Data act, CRA and other regulations.
- Clarify and reduce overlaps between EU legal acts in the digital field. Below are examples of clarifications raised by the business community:
    - Article 5 GDPR[6] principles for the processing of personal data. Adapt the principles of purpose limitation and data minimization to enable training of AI systems on large amounts of data. There is a need to clarify that it is permissible to "process" data for the

[6] Concerns that data must be collected for specific, explicitly stated and legitimate purposes and not subsequently processed in a way that is incompatible with these purposes. Further processing for archival purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) shall not be considered incompatible with the original purposes (purpose limitation).

purpose of making it anonymous and how this type of data may be used.

- Article 10 GDPR (processing of personal data relating to criminal convictions and offences) has been interpreted in Sweden as preventing the sharing of information about cyber threats (e.g. IP addresses used in threat activities). Guidance from the European level on how to interpret this article would be desirable.

- Article 22 GDPR.[7] There is a need to clarify how automated decision-making is to be applied to AI systems and when human intervention is sufficient as required by legislation.

Introduce more uniform and consistent criteria and requirements for reporting incidents

- Implement compliant thresholds, timelines, and criteria for reporting incidents to reduce administrative burden and increase regulatory compliance.

- Align incident reporting timelines with the GDPR timeline/hours model to allow for a thorough initial assessment prior to notification.

- Create a single, harmonised reporting template that applies under NIS2, CRA, GDPR and other related legal acts.

- Incident reporting needs to be simplified as new cybersecurity regulations are implemented. This can be achieved by developing clear and step-by-step rules for incident reporting and a one-stop-shop.

Let the CSA certification be valid for overlapping requirements

- Let CSA certification, when obtained voluntarily and when it meets relevant legal obligations, be valid for overlapping requirements of the CRA and NIS2. This is in order to avoid unnecessary repetition of assessments or audits.

[7] Concerns the right of the data subject not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

impl | Implementeringsrådet

- Maintain the principle of proportionality in the implementation of the CRA by maintaining the NLF and ensure that low-risk products continue to be subject to the possibility of self-monitoring, without extending certification requirements beyond what is strictly necessary.

Ensure cybersecurity regulations don't hinder data transfer or thwart global data flows

- Streamline and clarify the requirements of the GDPR, the Data act and the Data Governance Act to increase legal certainty around international data flows.

The contact person in this case is Investigation Secretary Veronica Götherström or Lena Nordqvist (förnamn.efternamn@regeringskansliet.se)

Decided by the Implementation Council on 25 August 2025.

This document has been machine translated from Swedish to English.