Cut and simplify – priorities of the electro and digital industry for a better competitiveness framework

ZVEI Position for an EU Digital Omnibus

The digital integration of the European single market holds immense potential for economic and social value creation. The companies of the electrical and digital industry are expected to generate two thirds of their turnover with digitally enhanced products and digital services by 2026. For them, the deeper integration of the European digital single market is a prerequisite for ensuring the future competitiveness of their businesses. However, companies across all industry sectors face significant challenges due to several regulatory issues, in particular: an increasing volume of regulatory measures, a lack of coherence between different legislations, overlapping or duplicate regulations and dysfunctionalities in European digital policy. These challenges not only lead to legal uncertainties and associated administrative costs but also to unnecessary competitive disadvantages compared to companies in non-EU countries.

Therefore, ZVEI welcomes the announcement of a digital package, the so-called “Digital Omnibus” to simplify EU digital regulations. ZVEI suggest the following measures in the areas of AI, cybersecurity and data usage to stimulate economic growth:

AI:

- **Slim down the AI Act**
  - Shift to sector specific regulation of Industrial AI
  - User orientation of the GPAI Code of Practice
  - Link transition periods to the availability of harmonised European standards
- **No need for an AI Liability Directive**

Cybersecurity:

- **Make the CRA suitable for industry**
  - Simplification of reporting and documentation obligations
  - Limitation of the free support period in the B2B area
  - Link transition periods to the availability of harmonised European standards
  - Introduce the concept of “benign products” under the CRA
- **Avoid redundancies in European cybersecurity legislation**

Data Usage:

- **Reform the GDPR**
  - The prohibition principle must be overcome
  - Clarification on the anonymization and pseudonymization of personal data
  - Clear distinction between B2C and B2B – remove bureaucratic burdens in pure B2B business
- **Slim down the Data Act**
  - Repeal B2B and B2C data sharing obligations (chapters II and III) - Data sharing obligations only in the event of market failure / power asymmetries
  - Limit cloud switching rules to Infrastructure as a Service Providers

AI

Slim down the AI Act

Shift to a sector specific regulation of Industrial AI

The European AI Act has been in force since 1 August 2024. Initial experience with the new regulation has already made it clear that the twin goals of minimising bureaucracy and providing legal certainty have not been achieved. Particularly in the area of Industrial AI, the AI Act creates serious hurdles and uncertainties that harm innovation and damage the competitiveness of European industry. Particularly serious from the perspective of ZVEI are the ambiguities and inconsistencies arising from Art. 6 (1) in combination with Annex I, Section A of the AI Act, which determines the high-risk AI criteria for products that are already regulated under other legal acts of the New Legislative Framework (NLF) (e.g. machinery, radio equipment and medical devices).

One example of a lack of congruence with NLF terminology is the divergent definition of “safety component” in the Machinery Regulation and the AI Act. As a result, many companies still do not know whether their products fall under the high-risk AI requirements of the AI Act; even checking whether a product is affected generates considerable effort and uncertainty. At the same time, the AI Act does not help to significantly promote safety and health goals, as this is already guaranteed in other NLF legislation that apply regardless of the use of AI in the product. **Products that are already covered by NLF legislation (Annex I, Section A) should therefore be exempted from the provisions of the AI Act**. Where it has not been done already, necessary AI-specific requirements should be integrated into the relevant NLF sector regulation without going beyond the requirements of the AI Act. Alternatively, it would be possible to integrate Annex I, Section A into Section B so that the products listed there also fall under the exemptions of Article 2 (2) of the AI Act.

User orientation of the GPAI Code of Practice

The General-Purpose AI Code of Practice not only affects providers of large language models (LLMs) but also has a significant impact on companies that integrate LLMs into their workflows and products. Depending on the interpretation of the AI Act, users of such models could suddenly find themselves in the role of “provider”. As such, they would have to comply with various obligations set out in Chapter V of the AI Act, including some that are difficult to fulfil without insider knowledge of the LLM**. The European Commission should ensure that compliance lies with the original providers of the LLMs and that fine-tuning rules are interpreted in a practical manner.** Otherwise, there is a risk that the potential of LLMs in industrial use will not be fully exploited.

Link transition periods to the availability of harmonised European standards

Due to the short transition period and the delay of the provision of harmonised European standards, companies do not have enough time to prepare for the implementation of the requirements of the AI Act or to place their products on the market in compliance with the AI Act. All other players involved in the implementation of a legal act (market surveillance authorities, notified bodies, national authorities) also face the challenge that suitable standards are not yet available and they need sufficient time for implementation[1]. **The deadlines for the application of the AI Act should be based on the publication of the harmonised European standards. A period of 24 months from publication is realistic for the industry to implement the standards.**

No need for an AI Liability Directive

From ZVEI’s point of view, there is currently no legal loophole and **no need for further regulation in the form of a separate AI liability directive**. The recently adopted new Product Liability Directive (EU) 2024/2853 has massively expanded the liability framework for software applications and artificial intelligence, and led to stricter rules. Additionally, there is the parallel applicable national tort law, which, in addition to product liability, also provides for the possibility of claims for damages caused by AI systems. **We therefore support the Commissions decision to withdraw the proposal of the AI Liability Directive**.

[1] See also ZVEI position paper “Ensure adequate transitions periods for a functioning EU Single Market”

Cybersecurity

Make the CRA suitable for industry

Simplification of reporting and documentation obligations

While the Cyber Resilience Act (CRA) prescribes the reporting of actively exploited vulnerabilities and serious security incidents via a central reporting platform, the NIS 2 Directive requires the immediate reporting of significant security incidents to the relevant CSIRT of the Member State. In order to avoid duplication of reporting obligations and unnecessary bureaucracy, **the CRA's central platform should be designed as a one-stop-shop solution for cybersecurity reporting**. Companies should be able to report security incidents within the scope of the NIS 2 Directive via this platform as well. This would reduce the operational burden without lowering the desired level of protection and at the same time contribute to the harmonisation of reporting obligations in the EU.

To ensure a proportionate and practicable implementation of the CRA, ZVEI recommends **aligning the applicability date of reporting obligations with the general CRA applicability date**. Additionally, the current requirement for an **early warning of actively exploited vulnerabilities within 24 hours should be removed**, as it merely involves indicating in which EU Member States the product was made available - information that can be provided without adverse effects during the subsequent 72-hour reporting phase. Furthermore, reporting obligations to ENISA, the CSIRT for actively exploited vulnerabilities or incidents (in line with Art. 14 (1) – (4), (6) and (7)) should not apply once the product's declared support period has ended.

The Annex VII of the CRA specifies detailed documentation obligations for manufacturers, forming a crucial component of the technical documentation required for demonstrating conformity. This annex has far-reaching implications, especially for manufacturers of non-important or non-critical products with digital elements, who will nonetheless face disproportionate obligations if no proportionality mechanisms are introduced. According to Art. 13 (7), manufacturers are obliged to "systematically document, in a manner that is proportionate to the nature and the cybersecurity risks, relevant cybersecurity aspects concerning the products with digital elements." At the same time, CRA Art. 33 (5) allows "Microenterprises and small enterprises may provide all elements of the technical documentation specified in Annex VII by using a simplified format.". This is where the Commission should come in and reduce the documentation requirements for manufacturers on a risk-based basis. ZVEI recommends that proportionality and risk relevance – especially in case of components – should be emphasized more clearly through interpretative guidelines. Furthermore, the **simplification measures for SMEs under Article 33(5) could be extended to all low-criticality products - regardless of manufacturer size - particularly for non-"important," and non-"critical" products with digital elements**. This approach would not only reduce unnecessary administrative burdens but also act as an active facilitator of bureaucratic relief.

The Commission is currently modernising several product legislations via a so-called "paperless omnibus initiative" to allow more digital documentation. However, the CRA is currently not part of this initiative. Although the CRA already permits some information to be provided online, the Omnibus proposal goes further, especially for B2B products. This creates a regulatory inconsistency that could force manufacturers to attach paper documentation to CRA-regulated products even where other legal acts no longer require it. The **CRA should therefore be included in the "paperless omnibus" to fully exploit digitalisation potential and avoid unnecessary burdens**.

Limitation of the free support period in the B2B area

During the support period of their product with digital elements, manufacturers are obliged to ensure that, where security updates are available, they are disseminated free of charge. Art. 13 (8) CRA prescribes to include other relevant Union law when determining the support period of products with digital elements. This can pose significant challenges to manufacturers. Regulations like the Machinery Regulation or the Ecodesign for Sustainable Products Regulation require manufacturers to define the lifetime of products. Many industrial products have physical lifetimes exceeding ten years, while their digital components follow much shorter innovation and support cycles. Requiring cybersecurity support for the entire physical lifetime imposes disproportionate burdens on manufacturers.

This challenge is particularly pronounced in B2B markets, where the duration and conditions of product support are typically defined by contractual agreements between business partners. These contracts reflect product-specific risk profiles, usage contexts and commercial terms, and offer a well-functioning and flexible framework

for defining support obligations - including the scope and cost of software updates. Imposing a statutory obligation to provide free updates during a predefined support period risks overriding these established contractual mechanisms and disrupting long-standing market practices.

We propose a **clear regulatory distinction between the physical and digital lifetimes of products with digital elements under the CRA**. We recommend introducing a "digital lifetime" concept, defined and transparently declared by the manufacturer, to allow for risk-based and economically viable support obligations. This would enhance legal certainty, promote sustainable product use, and maintain the competitiveness of Europe's high-tech industry - without compromising the CRA's cybersecurity objectives.

Link transition periods to the availability of harmonised European standards

To ensure the effective and practical implementation of the CRA, it is essential that the European Commission – in close cooperation with the European Standardisation Organisations (ESOs) as well as technical experts from industry and civil society – define and agree on realistic, technically sound timelines for the development and delivery of the harmonised European standards under the CRA. This applies in particular to the vertical, product-specific standards that enable the presumption of conformity with the essential requirements of the CRA. These standards are not merely implementation tools. Rather, they are an integral legal basis for demonstrating compliance, especially for products with digital elements classified as "important" under Annex III (Class I), where third-party conformity assessment would otherwise be mandatory. Given this, it must be ensured that **a minimum of 36 months elapses between the formal publication of the relevant harmonised standards** in the *Official Journal of the European Union* **and the end of the transition period of the CRA**. Only this timeframe provides manufacturers with the necessary legal certainty and operational feasibility to meaningfully integrate the CRA requirements into product development and production processes. All other players involved in the implementation of a legal act (market surveillance authorities, notified bodies, national authorities) also face the challenge that suitable standards are not yet available and they need sufficient time for implementation[2].

Tight implementation timelines risk negatively impacting existing supply chains. Most products with digital elements currently in use were developed before the adoption of the CRA - in parts as general-purpose components without alignment to specific, risk-based cybersecurity requirements. To achieve conformity with the CRA and to be placed on the market beyond December 11th, 2027, parts of these product portfolios would require significant redesign. For certain product types already on the market, timely adaptation may not be technically or economically feasible. This could result in the withdrawal of established products, with far-reaching implications for supply chain continuity and the availability of products with digital elements within the EU. Particularly withdrawals in the semiconductor sector could lead to severe implications as they serve as a foundational technology across a broad spectrum of applications. The link of transition periods to the availability of harmonized European standards and the introduction of the concept of "benign products" (see below) would mitigate this risk.

If such an extension cannot be granted, manufacturers of all "important" products with digital elements (Annex III CRA) should temporarily be permitted to use Module A (internal production control) as a conformity assessment procedure, until the vertical harmonised standards are available. This pragmatic interim solution would safeguard legal certainty and contribute to market continuity without compromising cybersecurity objectives. The CRA's reliance on the availability of harmonised standards as a precondition for using Module A has far-reaching consequences. In their absence, manufacturers are forced to involve a notified body, even where the product risk profile is low. This dependency has already led to severe delays under other EU legal acts – such as the Radio Equipment Directive – and is expected again under the CRA. It imposes unpredictable and disproportionate burdens on both manufacturers and notified bodies, particularly during transitional phases.

Introduce the concept of "benign products" under the CRA

The scope of the CRA will include also trivial products with digital elements like simple sensors, passive electronic components, or basic switching devices (e.g. analog-to-digital converter, electric toothbrushes barcode readers). Even though the CRA will not require any additional cybersecurity protection measures due to the virtually non-existent cybersecurity risks, these products with digital elements will still have to go through the NLF formal conformity assessment to demonstrate CRA compliance with all processes, documents, and

[2] See also ZVEI position paper "Ensure adequate transitions periods for a functioning EU Single Market"

labelling requirements. Consequently, without any lower limits for such "benign products," costs are generated that have no discernible benefit for the manufacturer, the customer or society.

To address this imbalance, **we propose introducing a specific exemption for "inherently benign products" under the CRA**. This category would apply to products that, due to their technical simplicity, cannot pose a cybersecurity risk. A precedent for such an approach exists in Recital 12 of the EMC Directive (2014/30/EU), which refers to products "inherently benign in terms of electromagnetic compatibility." A similar reference – "inherently benign in terms of cybersecurity" – would be appropriate and beneficial in the context of the CRA. To ensure legal certainty and prevent circumvention of the regulation, we propose the following definition:

> Article 3 (5a):
> *"benign product" means a product which cannot reasonably be expected to cause a cybersecurity risk because it is technically too limited to do so."*

Further clarification on the scope and application of this category could be provided through implementing guidelines or delegated acts, ensuring consistent interpretation and enforcement. Introducing this exemption would strengthen regulatory proportionality while safeguarding cybersecurity objectives.

Avoid redundancies in European cybersecurity legislation

A core objective of European digital policy must be the simplification and clarification of the EU's cybersecurity regulatory framework. At present, there are significant overlaps between horizontal regulations - such as the Cyber Resilience Act (CRA) or the Cybersecurity Act (CSA) - and existing vertical legislation, including the Radio Equipment Directive (RED) and the Machinery Regulation (MR). **From the ZVEI's point of view, the CRA should be the central product regulation in the cybersecurity sector.**

The CSA, originally intended as the cornerstone of a European cybersecurity certification framework, has fallen short in practice. Voluntary certification schemes like the EU Cybersecurity Certification Scheme on Common Criteria (EUCC) have seen limited industry uptake due to their complexity, narrow applicability, and slow implementation. The entry into force of the CRA marks a turning point: it establishes a mandatory, horizontal legal framework with binding cybersecurity requirements, including manufacturer obligations, essential requirements, and conformity assessment procedures for all products with digital elements. Maintaining both the CRA and the product-related certification framework under the CSA in parallel introduces regulatory fragmentation, legal uncertainty, and administrative overhead - without delivering additional value. **Certification requirements under the CRA** should therefore be phased in with care and **should be harmonized with existing CSA certifications**, in order to avoid time consuming, unnecessary and expensive double certification requirements. Ultimately, only one mandatory IT security certification scheme should be maintained.

Similarly, a redundancy exists between the CRA and the Delegated Regulation (EU) 2022/30 under the RED (Article 3(3) (d), (e), (f)), which also addresses the cybersecurity of connected products. Both frameworks aim to regulate the same risks. To protect investments taken by manufacturers and facilitate a smooth transition from RED Delegated Regulation to CRA product requirements, EC type examinations for directly internet connected products under the RED should be deemed sufficient for CRA product compliance, for default and important class 1 products for the validity of the RED type examination if issued before the date of application of the CRA. Furthermore, the Commission should plan for a **withdrawal of Delegated Regulation 2022/30 once the CRA becomes fully applicable**. A coordinated transitional period is necessary to prevent conflicting timelines, avoid regulatory discontinuities, and ensure a smooth transition for manufacturers.

Data usage

Reform the GDPR

The prohibition principle must be overcome

The protection of personal data and the individual's right to informational self-determination are of paramount importance and must remain guaranteed. Nevertheless, the exchange and use of data are essential for the European economy - especially the data-driven electrical and digital industry - in order to bring new technologies and innovations to the market and thus ensure sustainable value creation. Against this backdrop, **we are in favour of "enabling" data protection and suggest overcoming the fundamental prohibition principle of the GDPR**.

Clarification on the anonymisation and pseudonymisation of personal data

The anonymisation of personal data is an important tool for companies to be able to process (large amounts of) data without falling within the scope of the GDPR. Proper anonymisation is therefore essential for strong data protection. Anonymised data plays a major role not only in the areas of statistics and research. Especially in connection with new technologies, legally secure anonymisation will become even more important, e.g. in the training of AI systems. It is not clear how legally secure anonymisation must be designed, which severely restricts the activities of companies - especially SMEs. Clarifications in the article text of the GDPR - in the sense of "enabling" data protection - would be highly desirable here. **ZVEI suggests, that anonymisation is based on a relative understanding**, i.e. that anonymisation also exists if re-identification of the data subject is not completely excluded but is ruled out due to a disproportionately high effort. **In addition, it should be clarified that the anonymisation process itself is not processing within the meaning of the GDPR.**

Furthermore, the processing of pseudonymised personal data should also be further privileged. The explicit mention in recitals 28 and 29 of the GDPR makes it clear that pseudonymisation is a particularly important data protection instrument in the context of technical and organizational measures (TOM). This prominent position should be taken into account beyond the simple mention in Article 32(1)(a) GDPR. A corresponding clarification would be conceivable with regard the balancing of in the context of the "legitimate interest" permission (Article 6(1)(f)), for example via a (possibly rebuttable) presumption rule.

Clear distinction between B2C and B2B – remove bureaucratic burdens in pure B2B business

We advocate a **clear distinction between data processing in B2C and B2B business transactions.** Employees of a company must inform employees of the customer or supplier about the data processing or obtain consent as part of their professional activities because the respective employees of both companies are natural persons. This applies even though in such a case they are not acting as private individuals with their own liability and insolvency risk, but as the non-liable extended arm of a legal entity. For example, the buyer acting on behalf of a company does not buy the goods for herself personally, but for the organisation. In this respect, these employed persons are less in need of protection in the B2B environment, because transactions of obligation and disposal are a burden on the organization and not on the natural persons acting on behalf of the legal entity. Nevertheless, they are subject to the entire canon of obligations and documentation requirements, which once again presents companies with high bureaucratic burdens without added value for individual protected interests. **ZVEI suggests that GDPR does not apply in such pure B2B relationships.**

Slim down the Data Act

Repeal B2B and B2C data sharing obligations (chapters II and III) - Data sharing obligations only in the event of market failure / power asymmetries

ZVEI supports the overarching objectives of the Data Act to promote the exchange and use of data. However, the current approach, characterizing a uniform regulation for both B2B and B2C contexts within chapters II and III, alongside a highly simplified and impractical understanding of industrial data sharing, raises significant legal and technical uncertainties. In addition, the so called 'trade secret handbrake mechanism' with its required safeguards, such as technical or organisational measures are inadequate to ensure meaningful protection of trade secrets while the threshold requiring a high likelihood of serious economic damage in order to refuse a data access request is excessively high and impractical to meet in real-world scenarios. Consequently, companies may be incentivized to design their products in a more data-efficient manner, thereby undermining the very objectives the Data Act aims to achieve. In light of these concerns, **we strongly recommend the repeal of chapters II and III and the promotion of the voluntary nature of data sharing to serve as the default standard.**

Mandatory measures should only be considered in sectors where significant and persistent barriers are identified through comprehensive market analyses, public consultations, and robust economic evidence. This, for instance, is true for the automotive sector, where the European Commission has conducted comprehensive in-depth studies[3] which have identified a number of technical, legal and policy issues concerning access to vehicle-generated data and state that "policy makers could consider measures to promote more competition in these markets and reduce the OEMs monopolistic hold on car data and service delivery channels". In this case, the Data Act should be applied to address the proven market asymmetries. The European Commission should not introduce new obligations, modify the core rights and duties, or impose requirements that goes beyond the current regulatory framework. An assessment of the measures implemented under the Data Act must be carried out within five years to determine whether the intended effects have been achieved. The European Commission should draw lessons from the evaluation results, particularly if it considers extending data-sharing obligations to other sectors.

Limit cloud switching rules to Infrastructure as a Service Providers

According to the prevailing interpretation of the Data Act's definition "data processing services", the regulation applies to all types of cloud-based products and solutions, despite significant differences in their value propositions and technical characteristics. Infrastructure as a Service (IaaS) typically delivers generic computing resources with a relatively high degree of standardisation with generic infrastructure and development environments where interoperability is technically feasible and economically viable through open interfaces and APIs. In contrast, Plattform as a Service (PaaS) and Software as a Service (SaaS) differ significantly in their complexity and integration depth. SaaS applications in B2B environments are highly customized, deeply integrated into business processes, and technically diverse. PaaS offerings provide development and runtime environments that are tailored to specific programming models, deployment workflows, and automation requirements. These platforms often involve tightly coupled services such as databases, application runtimes, and orchestration layers, which are not easily interchangeable across providers. Similar to SaaS, PaaS services are deeply embedded in application development lifecycles and enterprise-specific tooling. Both the interoperability requirements under Art. 30 and the contractual switching framework established under Art. 25 make it difficult to sustain long-term business models for SaaS and PaaS solutions, including multi-year contracts. Due to unique data models, workflows, and user interactions, SaaS and PaaS solutions cannot be made interoperable or portable without substantial investments - often at the expense of functionality and security. This can hinder investments and limit the emergence of potential new offers. Therefore, **we strongly recommend restricting the cloud switching provisions to infrastructure service providers (IaaS) and explicitly excluding Software as a Service (SaaS) and Platform as a Service (PaaS) from the regulation's scope.**

[3] Study on access to in-vehicle data and resources; McCarthy, M., Seidl, M., Mohan, S., Hopkin, J., Stevens, A., Ognissanto, F; 2017 and 'Access to digital car data and competition in aftersales services', JRC Digital Economy Working Paper 2018-06, Bertin Martens, Frank Mueller-Langer, 2018.

Contact
Jochen Reinschmidt • Director • Division Digitalisation & Law •
Phone: +49 30 30696023 • Mobile: +49 174 9414 164 • Mail: Jochen.Reinschmidt@zvei.org

ZVEI e. V. • Electro and Digital Industry Association • Charlottenstrasse 35/36 • 10117 Berlin • Germany
Lobbying Register ID.: R002101 • EU Transparency Register ID: 94770746469-09 • www.zvei.org

Date: June 19, 2025