Berlin, December 14th 2022

Verband kommunaler Unternehmen e.V.
Invalidenstraße 91
10115 Berlin

www.vku.de

BDEW Bundesverband der Energie- und Wasserwirtschaft e. V.
Reinhardtstraße 32
10117 Berlin

www.bdew.de

Remarks

Cyber Resilience Act

Position Paper of the German Energy and Water Industries and Local Public Utilities

EU Transparency-Register-ID BDEW: 20457441380-38
EU Transparency-Register-ID VKU: 1420587986-32

The **German Association of Energy and Water Industries (BDEW)** and its regional organisations represent over 1,900 companies. The membership comprises both privately and publicly owned companies at the local, regional and national level. They account for around 90 percent of the electricity production, over 60 percent of local and district heating supply, 90 percent of natural gas, over 90 percent of energy networks and 80 percent of drinking water extraction as well as around a third of wastewater disposal in Germany.

The **German Association of Local Public Utilities „Verband kommunaler Unternehmen" (VKU)** represents over 1,500 local public utilities in Germany, operating in the sectors of energy, water/waste water, waste management and telecommunication. In 2019, VKU's members, which have more than 283,000 employees, generated a turnover of around 123 billion euro of which more than 13 billion euro were reinvested. In the end-customer segment, VKU's member companies have a market share of 62 percent in the electricity market, 67 percent in the natural gas market, 91 percent in the drinking water sector, 79 percent in heating supply market and 45 percent in waste-water disposal. Every day, they dispose of 31,500 tons of municipal waste through separate collection and take a vital role in ensuring recycling rates of 67 percent, which rate the highest within the EU. Additionally, more and more local public utilities are committed to the deployment of broadband infrastructure. 203 members invest more than 700 million euro every year. When deploying broadband infrastructure, 92 percent of local public utilities rely at least on fibre to the building.

I. Security by Design to be welcomed, but availability of critical components crucial

BDEW and VKU welcome and support the security by design approach proposed by the Cyber Resilience Act. Only through this approach, and in the context of the increasing importance of attacks in the supply chain and the growing geopolitical implications in the procurement of IT components, can security be guaranteed in the future. However, security by design must not become the bottleneck of an already difficult procurement process. In this respect, the requirements arising from the security by design approach should also create the industrial policy framework conditions for digital and technological sovereignty in the European Union.

BDEW and VKU are pointing out that there is a limited number of manufacturers and solution providers of essential components of process and automation technology which are used in the energy and water industries. After all, the availability of critical components is also decisive for the security of supply itself. Especially in the case of highly critical products, certification obligations would likely have the consequence that the diversity of suppliers could possibly be limited to a few manufacturers worldwide. In the context of the efforts to achieve technological sovereignty in the European Union, the political and regulatory framework must ensure that a sufficient number of trustworthy European manufacturers of relevant products, services and processes is guaranteed at all times. A sector-specific certification obligation must not lead to dependence on manufacturers from non-EU countries. In addition, it can be assumed that such a certification obligation would result in rising prices for the components concerned, which in turn could have cost effects in the supply of energy and drinking water as well as the disposal of wastewater.

II. Artikel 10:

Article 10 para. 6 reads as follows:

> *“When placing a product with digital elements on the market, and for the expected product lifetime or for a period of five years from the placing of the product on the market, whichever is shorter, manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I.”*

Following this Article there is a fixed five-year limit for the manufactures to ensure that vulnerabilities of a product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I. This includes e.g. the obligation to provide security updates. Only if the expected lifetime (in the CRA also called “life cycle”) of the product is shorter, then this shorter lifetime of the product is relevant (see as well Article 10 para. 12 and Article 23 para. 2). This restriction clearly goes against one of the main goals of the Cyber Resilience Act.

One of the goals of the Cyber Resilience Act is to lay down essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle, and obligations for economic operators in relation to these processes (Article 2 lit. c). This Article states clearly that the cybersecurity of the products shall be ensured during the whole life cycle / lifetime of the product.

Whereas in the field of consumer products the fixed five years limit might be sufficient, it is not appropriate in the industry context. Especially in the context of energy supply companies and other forms of essential and important entities as stated in the NIS 2-Directive (2020/0359), the fixed five years limit is too short. These kinds of companies often buy products / machines, which are typically used for several decades. Limiting the obligations of the manufacturers to five years could lead to serious security problems, as well as the need to regularly replace functioning components.

Especially in the context of essential and important entities, there should not be a fixed limit to the obligation to handle the vulnerabilities of a product effectively and in accordance with the essential requirements set out in Section 2 of Annex I during the whole expected/typical life cycle of the product. We recommend differentiating between "normal" products with digital elements, "critical product with digital elements" and "highly critical product with digital elements". In particular, the long amortization periods of several decades for operational technology and secondary technology, especially in the energy industry, must be taken into account when determining the duration of manufacturer obligations in the context of high-critical products.

III. Artikel 11: Incident Reporting

BDEW and VKU welcome and support extended reporting obligations for manufacturers. However, the reporting obligations must be appropriate so that possible vulnerabilities can be sufficiently verified beforehand. In addition, Responsible Disclosure must be ensured.

IV. Artikel 16:

Article 16 should read as follows:

> *"A natural or legal person, other than the manufacturer, the importer or the distributor, that carries out a substantial modification of the product with digital elements* ***and places the product on the market / makes the product available on the market*** *shall be considered a manufacturer for the purposes of this Regulation.*
>
> *That person shall be subject to the obligations of the manufacturer set out in Articles 10 and 11(1), (2), (4) and (7), for the part of the product that is affected by the substantial modification or, if the substantial modification has an impact on the cybersecurity of the product with digital elements as a whole, for the entire product."*

Especially in the context of energy supply companies, it is common that security products are modified by the buyer company to meet their own needs. In many cases, especially with software, it is simply necessary to adapt them to the IT and security environment. As these products are not sold on the market, but strictly for internal use, the company operating them should not be faced with obligations similar to those for placing such products on the market. As proposed by the Commission, Article 16 could lead to exactly such an outcome, where buyer companies would be obliged to fulfill the requirements of Article 10, 11 (1), (2), (4) and (7). **To mitigate such a scenario, Article 16 should be limited to legal persons who are placing products on the market / making products available on the market.**

Most of obligation set out in these Articles are clearly designed for products, which are sold on the market. E.g. Art. 11 (4) states:

> *"The manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements about the incident and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the incident."*

If a company modifies a product only for itself and does not place it on the market / make it available on the market, there is no different user this company could inform.

In addition, Article 15 already covers all other economic operators who are placing the product on the market after a substantial modification (importer and distributor). This is already sufficient to secure the supply chain of digital products. Additional obligations for the buyer companies would not be adequate for their role and responsibilities regarding the supply chain.

Furthermore, it should be clarified that there is no "placing on the market" / "making available on the market", if a product is only distributed within a "group of undertakings". A group of undertakings shall mean a controlling undertaking and its controlled undertakings.

V. Annex 2, Chapter 2

For responsible disclosure, updates to known vulnerabilities should be made available immediately by manufacturers, but this should not lead to publication of the vulnerability itself. Details of vulnerabilities should generally not be made public immediately after being discovered by the manufacturer, because potential attackers can exploit these vulnerabilities.

In addition, consistent and uniform terminology must be established between the Cyber Resilience Act and Annex II. Currently, the Cyber Resilience Act defines digital products from the perspective of consumer products and thus does not adequately address the requirements of Class II and high-critical digital products described in Annex II.

Contact

Mathias Böswetter
Berlin Headquarters
Phone: +49 30 300199 1526
mathias.boeswetter@bdew.de

Sandra Struve
BDEW Representation to the EU
Phone: +32 2 774 5110
sandra.struve@bdew.de

Contact

Wolf Buchholz
Berlin Headquarters
Phone: +49 30 58580-317
buchholz@vku.de

Simon Kessel
VKU Office Brussels
Phone: +49 170 8580 125
kessel@vku.de