ZVEI:
Die Elektroindustrie

Shaping digital change. Building trust.

# Guidelines of the electrical industry for the responsible use of data and platforms

Version 2.0

German Electrical and Electronic Manufacturers' Association

ZVEI:
Die Elektroindustrie

**Guidelines for the responsible use of data and platforms in the electrical industry**

Published by:
ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.
German Electrical and Electronic Manufacturers' Association
Innovation Policy Department
Charlottenstraße 35/36
10117 Berlin, Germany

Responsible: Jochen Reinschmidt
Phone: +49 30 306960-23
E-mail: jochen.reinschmidt@zvei.org

www.zvei.org

January 2020

# Preliminary remarks

Digitalization brings a fundamental structural change to both the economy and society. The German electrical industry interlinks with its products and solutions the analogue and digital worlds and is actively shaping this change. The digitalization of the economy is the prerequisite for stable and sustainable growth. It creates value for society and contributes to solving global challenges. Digital economy in the industrial sector means establishing the connectivity of both individual products and entire infrastructures that can extend beyond companies and include suppliers and customers.

The „raw material" of the digital economy is data. Today, companies in the electrical industry use data primarily to optimize existing business models and processes. Increasingly however, data is also being used to develop new business models. This creates new value creation structures and partner networks. Digital platforms also play a particularly important role in the industrial context. They are the hubs where market players use and exchange data. Open platforms offer small and medium-sized enterprises (SMEs) and start-ups the opportunity to become involved in newly emerging ecosystems. But the use and processing of data and the operation of platforms can also lead to misuse and conflicts.

In order to be able to use the potential of data and platforms, next to clear legal regulations, the development of trust is necessary. This requires a common basis of fundamental values that is consistently implemented in practical action.

In Germany and Europe, the focus is always on the human being together with the fundamental rights derived from the protection of human dignity. Regarding data and platforms, the protection of privacy and the protection of personal data are of particular importance. Our foundation of common values also includes the rules of the social market economy, which define fair competition, and the implementation of the Sustainable Development Goals of the United Nations. This is the value proposition of the electrical industry: values that guide our actions and which we promote in international business competition.

Based on this value foundation, the present guidelines set out in concrete terms what the electrical industry is guided by when using data and designing platforms. We regard the formulation of the guidelines as a continuous process and an invitation for discussion. Based on these guidelines, we will play an active role in the dialogue on the framework conditions of the digital economy. The guidelines are being implemented concretely, as illustrated in the examples from the corporate practice of ZVEI member companies in the appendix.

# Ten guidelines for the responsible use of data and platforms

## 1 Personal data is worth of particular protection

Companies in Germany's electrical industry consider the individual's self-determination of their own data a central basis for the digital economy. We see the requirements for data protection set out in the General Data Protection Regulation (GDPR) as a competitive advantage in the global competition.

## 2 Enabling fair access to data

In principle, each generator of data should be able to decide how to handle the data it generates. ZVEI rejects the monopolization of data and the creation of new legislation for data ownership rights. Access to and use of data should be organized between partners freely and in fair contracts that take the interests of both sides into account in an appropriate manner. This ensures that customers and business partners can determine and control which data is accessed and for what purpose it is used.

## 3 Promoting data security through security by design and security lifecycle management

Basic requirements for the sharing and use of data are: Access that is protected against misuse; secure processing, storage and handling of data; and the maintenance of its integrity and confidentiality. Companies in the electrical industry are therefore committed to promote security as comprehensively as possible through a holistic approach. This includes both security by design in the development phase and security lifecycle management throughout the entire product and data lifecycle.
Unauthorized access must be countered with the fastest possible response.

## 4 Treat value added derived from data as an economically significant asset of enterprises

Digital value creation is based substantially on the processing and evaluation of data, for example through data analysis techniques or the application of artificial intelligence. We consider digital value creation through data processing and evaluation as an economically significant asset worthy of protection. This creates an incentive for innovation and at the same time protects investments.

## 5 Supporting the portability and interoperability of data used for competitive purposes

The companies in Germany's electrical industry actively promote competition. The ability to use data across different generation and application contexts in parallel can be achieved by supporting data portability through interoperable data formats and information models based on freely accessible standards. In this way, data exchange or data pooling between different providers is possible, thus promoting competition.

## 6 Promoting the sustainable use of data

ZVEI is committed to the widest possible access to and sustainable use of non-personal data or anonymized data for the common good of society and for achieving global sustainability goals. Due consideration must be given at the same time to economic interests and the costs associated with the provision of the data.

## 7 Enhancing open innovation and co-creation

In the data-driven digital economy, value chains become flexible value creation networks with new partner constellations. New business models often go hand in hand with changing constellations of actors and are often embedded in newly emerging ecosystems. These offer start-ups, SMEs and large companies' opportunities to participate jointly in digital value creation. In this context, the protection of the intellectual property of the respective partners must be ensured.

In order to support the development of such ecosystems, ZVEI is committed to new forms of cooperation and approaches such as open innovation and co-creation, in which the customer or supplier becomes the innovation partner.

## 8 Enable participation in digital platforms

Industrial platforms should provide non-discriminatory access to all interested parties. Quality standards or technological prerequisites may have to be defined to ensure security and functionality of the platform (for example by the certification of components); however, these must not be unilateral at the expense of individual market participants.

## 9 Promoting transparent operation of digital platforms

A platform interconnects different stakeholders, which can pursue different interests. This also includes the operator of the platform. The platform operator has the task of making these interests as transparent as possible to all platform users. This is particularly the case when the content or functionality of the platform are influenced by the interests of individual actors, such as the order of search results.

By the provision of suitable opt-in/opt-out functions, platform users should be given the opportunity to track and control the use and exploitation of the data they contribute in the platform operation in a differentiated manner.

## 10 Enabling fair competition between digital platforms

Member companies ZVEI are actively committed to fair and innovation-promoting international competition between platforms. The design of platforms should therefore prevent the creation of anti-competitive lock-in mechanisms that artificially obstruct users from switching to other platforms. In particular, the migration capability of data should be ensured, and the simultaneous use of multiple platforms should be made possible.

# Attachement:
# Case studies from ZVEI member companies

## 1 Personal data is worth of particular protection

### Case study 1:

Befund24 has set up a marketplace for the mediation of remote diagnosis services in the health sector. To protect personal data, the platform operates according to the basic principle of „privacy by design and by default" in accordance with Article 25 of the General Data Protection Regulation (GDPR). The development of the Befund24 marketplace solution is based on the Siemens Healthineers cybersecurity development process, which includes a threat and risk analysis (TRA), the implementation of security standards and security checks. In addition, external penetration tests are carried out regularly. Patient data is always encrypted in the Befund24 cloud. Patients can assert any claims for information against the hospital or the creator of the findings report.

Further Information: https://www.befund24.de/

### Case study 2:

In future, Bundesdruckerei will offer data trustee services in the healthcare sector (pseudonymisation, authorisation and consent management) as a service via a digital platform. With the help of a trusted third party, personal data and pseudonyms can be managed securely. Only pseudonyms are assigned to the user data. By means of an authorization management the data provider can decide who receives which data for inspection or revoke this authorization.

Further information: https://www.bundesdruckerei.de/de/Themen-Trends/Magazin/Der-Datentreuhaender-als-neutrale-Schutzinstanz

### Case study 3:

Eaton has introduced a uniform, company-wide policy for personal data protection. Since the Group operates globally, and there is no robust international legislation on personal data protection, Eaton has introduced a policy that applies to all sites and subsidiaries worldwide and is based on the General Data Protection Regulation (GDPR). This is intended to ensure that the personal data of customers and employees worldwide is handled in accordance with the highest security standards currently available.

Further information: https://www.eaton.com/content/eaton/us/en-us/company/policies-and-statements/privacy-cookies-and-data-protection.html

### Case study 4:

Siemens is implementing a uniform data protection solution for MindSphere worldwide, which was developed in accordance with the standards of the General Data Protection Regulation (GDPR). With MindSphere Data Privacy Terms, every customer is offered the conclusion of contractual clauses that give them full control over the content with personal data processed on MindSphere. This includes transparency of all sub-service providers used with access to personal data and audit rights in order to be able to check compliance with contractual promises and data protection requirements. The MindSphere Data Privacy Terms apply worldwide and thus enable compliance with European data protection law as well as local data protection requirements in other jurisdictions.

Further information: https://www.plm.automation.siemens.com/media/global/en/Siemens_MindSphere_Whitepaper_tcm27-9395.pdf

## 2 Enabling fair access to data

### Case study 1:

Bundesdruckerei offers itself as a trusted partner to facilitate the exchange of data between organisations. This is because if organisations do not fully trust each other when exchanging data or if direct data exchange is not technically or legally possible, this can prevent the development of data-driven business models. As a trusted partner of both organizations, the data trustee intervenes in between. The original data is transferred to the data custodian and analysed and processed according to the agreed data governance. Only the result is passed on to the authorised organisation.

Further information: https://www.bundesdruckerei.de/de/Themen-Trends/Magazin/Der-Datentreuhaender-als-neutrale-Schutzinstanz

### Case study 2:

Osram has established the Lightelligence software platform, which enables cloud-based collection and analysis of a wide range of data from various sources. Only the respective customers themselves have control over their data. A granular, transparent authorization concept ensures that data is not released to third parties unintentionally. In addition, it is possible to give the applications of third parties only those rights that are necessary for their function. There is a strict separation between individual customers, which is verified by various technical measures and tested regularly. Osram does not access or use customer data for its own purposes.

Further information: https://www.lightelligence.io/

## 3 Promoting data security through security by design and security lifecycle management

### Case study 1:

Befund24 has set up a marketplace for the mediation of remote diagnosis services in the health sector. To protect personal data, the platform operates according to the basic principle of „privacy by design and by default" in accordance with Article 25 of the General Data Protection Regulation (GDPR). The development of the Befund24 marketplace solution is based on the Siemens Healthineers cybersecurity development process, which includes a threat and risk analysis (TRA), the implementation of security standards and security checks. In addition, external penetration tests are carried out regularly. Patient data is always encrypted in the Befund24 cloud. Patients can assert any claims for information against the hospital or the creator of the findings report.

Further Information: https://www.befund24.de/

### Case study 2:

At Eaton, every digitally controlled or networked product or system is tested by a global Center of Excellence (CoE) for product cybersecurity as part of the cybersecurity life-cycle before being launched to the market. The CoE, together with the product managers, acts as an approval body.

Further information: https://www.eaton.com/us/en-us/markets/innovation-stories/Managing-Cybersecurity-Risks.html

### Case study 3:

The high safety requirements for automated and networked vehicles have a major influence on the design of Infineon chips as the smallest electronic elements in the vehicle. In modern vehicles with 100 or more ECUs, so-called security anchors protect against manipulation or theft of data. These semiconductor chips with highly secure encryption mechanisms are either directly integrated into the numerous microcontrollers or built in as discrete security controllers. These chips protect against manipulation and intrusion attempts, so that a violation of data security can be fended off.

Further Information: https://www.infineon.com/cms/en/discoveries/trusted-driving/

### Case study 4:

Phoenix Contact takes security requirements for software and hardware into account as early as the development phase of a product. For automation solutions, a security concept with the necessary protective measures is developed. Both are carried out in accordance with the international IEC 62443 series of standards. Phoenix Contact has also established a team as a contact partner for users who discover security gaps and actively informs them about known safety gaps. The Product Security Incident Response Team (PSIRT) adheres to the process chain of the standard series when processing, evaluating and publishing reports and updates.

Further information: https://www.phoenixcontact.com/online/portal/pc/pxc/offcontext/insite_landing_page/!ut/p/z1/xZRRb4IwFIV_DY

### Case study 5:

Siemens has established ten principles for cyber security in its „Charter of Trust". These include the principle of „Taking Responsibility in the Digital Supply Chain". This means, for example, that security must also be anchored in the value network with suppliers. To ensure this, a roll-out was started, which includes corresponding terms and conditions in all purchasing contracts and the qualification of 300 pilot suppliers. Siemens supports business partners and suppliers in implementing the „Roadmap to Compliance" with the necessary security levels, including external certification.

Further information: https://new.siemens.com/global/en/company/topic-areas/cybersecurity/charter-of-trust.html

## 4 Treat value added derived from data as an economically significant asset of enterprises

### Case study 1:

The ABB Ability™ Collaborative Operations Centers (COC) offers a new form of cooperation in digital services. ABB experts use secure cloud-based applications with which they collect, combine, analyze and visualize plant data 24/7 up to proactive reporting, depending on the scope of services. Customers can thus fast and efficiently obtain decision documents to improve their plant availability, production throughput or product quality, thus increasing their cost efficiency and the performance of their operating processes. Mass data from the plants or fleets is linked with in-depth industry-specific knowledge. The aim is to create new value creation potential together with customers.

Further information: https://new.abb.com/news/detail/4357/abb-ability-collaborative-operations-center-unterstuetzt-die-industrielle-automatisierung

### Case study 2:

One example of value added derived from data is data-based condition-based maintenance, which allows the condition values of a field device to be analyzed in the central maintenance management system.

If operating data is collected from a fleet of machines, data analysis can be used to determine sensible maintenance times. The underlying evaluation procedures can be protectable. Siemens holds patents for this in the area of „Systems and methods for condition-based maintenance".

## 5 Supporting the portability and interoperability of data used for competitive purposes

### Case study 1:

ABB supports the development of the Asset Administration Shell concept and incorporates it into its own device and platform developments. The Asset Administration Shell allows data and services from IIoT devices to be connected via a unified interface, regardless of the device manufacturer. In addition, device properties can be exchanged across manufacturers in a standardized way using eCl@ss.

Further information: https://www.youtube.com/watch?v=AXQ0yIonNxk&t=1s

### Case study 2:

In 2018, Infineon launched a so-called Trusted Platform Module (TPM) specifically for automotive applications. The external communication of a vehicle is protected by the TPM - a kind of vault - which generates, stores, distributes and manages cryptographic keys, for example. The TPM complies with international standards (ISO/IEC 11889) and thus contributes significantly to the portability and interoperability of data.

Further information: https://www.infineon.com/cms/en/product/security-smart-card-solutions/optiga-embedded-security-solutions/optiga-tpm/sli-9670/

### Case study 3:

Siemens MindSphere offers open, bi-directional communication at every interface and can be integrated with applications, machines, enterprise IT systems and other IT platforms. Customers also have the option of designing the data models according to their own wishes or removing data from the backend. With IDL (Integrated Data Lake) and EDI (Enterprise Data Interconnect), Siemens also offers a methodology for using data from other data lakes for MindSphere applications without changing their storage location.

Further information: https://www.plm.automation.siemens.com/media/global/en/Siemens_MindSphere_Whitepaper_tcm27-9395.pdf

## 6 Promoting the sustainable use of data

### Case study:

BLIDS, the Lightning Information Service from Siemens, locates lightning storms in Germany and other European countries.

In addition to the paid subscription, the BLIDS spy provides a set of free overview thunderstorm maps for Germany and other European countries. Based on over 155 measuring stations distributed throughout Europe, lightning strikes can be located with an accuracy of up to 200 meters. Siemens will provide an updated map every 15 minutes via BLIDS Spion, showing all lightning strikes of the last two hours.

Further information: https://new.siemens.com/global/de/produkte/services/blids.html

## 7 Enhancing open innovation and co-creation

### Case study 1:

ABB supports its customers in the digitalization of business processes. In co-creation workshops, customers can transform their ideas into digital solutions together with the respective ABB business units. The workshops are tailored for each customer depending on the industry, topic and problem definition. The customer is involved in the innovation process right from the beginning by means of „Design Thinking“. The newly developed solutions and business models can thus be tested more easily.

Further information: https://new.abb.com/news/detail/18797/lets-shape-the-digital-world-of-the-future-together

### Case study 2:

Phoenix Contact has set up an open webstore for solutions from various suppliers for the PLCnext control platform. The PLCnext Store provides software applications with which interested parties can functionally expand a PLCnext controller and then offer it for sale. The PLCnext Store provides users with a variety of apps - from software libraries for accelerated programming to pre-programmed apps that do not require programming knowledge to use.

Further information: https://www.plcnextstore.com/

## 8 Enable participation in digital platforms

### Case study 1:

In future, Bundesdruckerei will offer data trustee services in the healthcare sector (pseudonymisation, authorisation and consent management) as a service via a digital platform. With the help of a trusted third party, personal data and pseudonyms can be managed securely. Only pseudonyms are assigned to the user data. By means of an authorization management the data provider can decide who receives which data for inspection or revoke this authorization.

Further information: https://www.bundesdruckerei.de/de/Themen-Trends/Magazin/Der-Datentreuhaender-als-neutrale-Schutzinstanz

### Case study 2:

Protiq offers an open platform for 3D printing. The digital business model of the manufacturer of 3D printing in plastic, ceramics and metal involves the customer configuring, ordering and paying online. Protiq also operates an open portal where various service providers can offer their 3D printing services. On the marketplace, the customer is free to choose which service provider should complete his order.

Further information: https://www.protiq.com/en/protiqmarketplace/

### Case study 3:

Third-party vendors are enabled to develop their own data-based business models through non-proprietary access to the Siemens MindSphere platform. For this purpose, third-party providers can use open interfaces and flexible connectivity solutions for machines (cross-vendor and with any protocols or communication standards) as well as for various software systems (e.g. ERP, MES):

In addition, the MindSphere Store will provide third parties with a secure distribution platform for industrial applications and digital services.

Further information: https://www.plm.automation.siemens.com/media/global/en/Siemens_MindSphere_Whitepaper_tcm27-9395.pdf

## 9 Promoting transparent operation of digital platforms

### Case study 1:

The ABB Ability™ Data Manifesto serves as a starting point for discussions about new digital solutions and is intended to form the basic values for a trustful cooperation in digitalization. It describes three aspects that customer data are not becoming the property of ABB, that the customer always knows what ABB is doing with their data, and that the data are not passed on without the explicit consent of the customer, regardless of whether it is personal data or machine data.

Further information: https://www.forbes.com/sites/abb/2017/04/13/a-call-to-action-for-the-internet-of-things-industry-lets-write-a-data-bill-of-rights-for-cloud-customers/#379899109a21

### Case study 2:

Protiq offers an open platform for 3D printing. The digital business model of the manufacturer of 3D printing in plastic, ceramics and metal involves the customer configuring, ordering and paying online. Protiq also operates an open portal where various service providers can offer their 3D printing services. On the marketplace, the customer is free to choose which service provider should complete his order.

Further information: https://www.protiq.com/en/protiqmarketplace/

## 10 Enabling fair competition between digital platforms

### Case study:

ABB supports the development of the Asset Administration Shell concept and incorporates it into its own device and platform developments. The Asset Administration Shell allows data and services from IIoT devices to be connected via a unified interface, regardless of the device manufacturer. In addition, device properties can be exchanged across manufacturers in a standardized way using eCl@ss.

Further information: https://www.youtube.com/watch?v=AXQ0yIonNxk&t=1s

ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e.V.
German Electrical and Electronic Manufacturers' Association
Lyoner Straße 9
60528 Frankfurt am Main, Germany

Phone: +49 69 6302-0
Fax: +49 69 6302-317
E-mail: zvei@zvei.org
www.zvei.org