# Joint position

## "Industrie du Futur - Industrie 4.0: The Digitisation of Industry at the Heart of our Economy and Society"

Joint Position
6th of July 2016, Paris

Once again, the French-German partnership has the potential to become the engine for our common European project: the digitisation of industry at the heart of our economy and society.

With respect to the developing European Digital Single Market, the French-German cooperation on Europe's digital agenda has constantly given significant impulses over the last months. In October 2015, a common declaration has been signed by the French Minister of Economic Affairs Emmanuel Macron and his German counterpart Sigmar Gabriel supporting a European Digital Single Market and intensifying French-German collaboration on research, innovation and business development. Only few months later, at the Hannover Fair 2016, the French national platform Alliance Industrie du Futur and the German Plattform Industrie 4.0 have agreed on a shared action plan of cooperation to improve pooling and sharing of national digital capabilities.

Based on these past French-German efforts, the Federation of Electrical, Electronic and Communication Industries (FIEEC) and the German Electrical and Electronic Manufacturers' Association (ZVEI) want to reaffirm this digital partnership by giving impulses and guidance to political decision makers. The French and German Electrical and Electronic Industries are a major, dynamic and innovative industrial sector of excellence in Europe. FIEEC and ZVEI are representing more than 4 600 companies of the manufacturing and engineering industries with

1,249 million employees and 278.5 billion euros of annual turnover. Membership encompasses global leaders as well as globally active small and medium size enterprises. As users and technology suppliers, our industries play a unique leadership role in the digital transformation of the European economy and society. This transformation process embodies great opportunities as well as various challenges, which need to be addressed effectively and in a collaborative manner. FIEEC and ZVEI are strongly persuaded that national initiatives such as Industrie du Futur in France and Industrie 4.0 in Germany are forward-looking projects to bundle capacities, while creating a fruitful environment of sharing best practices and innovation. At the same time, we need more cross-border and European cooperation of these national projects to face common challenges and to avoid fragmentation. The French-German cooperation on the digital transformation is one of the most promising bilateral synergies across the European Union and is a lighthouse partnership program for other Member States.

Our industries highlight the importance of an ambitious European industrial digital strategy, which should ensure an adequate regulatory framework that allows economic growth, creates new jobs, and speeds up market-driven innovations. Moreover, on behalf of our member companies, both associations are strongly committed to send a clear message to European decision makers to take industrial stakeholders into account for making full use of Europe's digital potentials. With respect to this industrial perspective, both associations agree on the following points addressing the regulatory framework for digitising Europe's industry, guidelines on the responsible use and management of data, the urgent need of a European cybersecurity strategy as well as open and industry-driven standard setting procedures.

## Executive Summary

FIEEC and ZVEI decided to work closely on common objectives and challenges of the digital transformation of our industries. Therefore, FIEEC and ZVEI have agreed on several joint messages and positions:

- Both industry associations are strongly committed to a further development and harmonisation of the European Digital Single Market.
- Cross-border cooperation is essential in order to avoid fragmentation and digital silo structures within European Member States.
- We want to create trust and confidence in a digital future by a regular and open dialogue with any stakeholder involved.
- The needed level of trust and confidence can only reached via a secure and safe data and cybersecurity infrastructure.
- We strongly believe that existing and future policy decisions applying to any field should take the dynamic process of the digitisation into account.
- The concept of digital self-determination is a guiding principal to guarantee responsible management of personal and non-personal data.
- Cybersecurity is a prerequisite of the digital transformation. Therefore, we want to promote the concept of industrial security (security-by-design security) in company with IT-security.
- The standardisation procedures concerning cyber-physical products, processes and services are rapidly changing. We need open, close-to-the-market, industry-driven standards which apply to the global market.
- An efficient market surveillance to create a level-playing field with our non-European competitors is also a major issue for our industries.

## 1. Digitising our Industries

The digitisation of our industries is a key priority on the national, European and global agenda. The internet of things has multiple implications and major effects on products, processes and services. The bigger picture shows that European electronic and electrical industries are holding leadership positions in producing and applying digital technologies. Our companies are users and suppliers of digital products. A future digital scenario, in which our industries are keeping this world-leading position, requires a clear vision about objectives and specific industry needs. One of the most important objectives is the evolvement and further harmonization of the European Digital Single Market. The full harmonisation would not only bring additional growth, jobs and investments to Europe's economy, but also an additional revenue to Europe's industry as €110 billion of revenue per annum could get capitalised. Europe's manufacturing industry is an essential cornerstone of our economic strengths and global competitiveness. Product quality and European standards are at high level. The electrical engineering industry in particular is a trendsetter for technological progress and innovation. This is why our industry needs to be better heard in the political process. We are a strong partner for building a digital Europe, to support our economies and to make them more competitive on the global market. Both, FIEEC and ZVEI are standing united to tackle challenges and to make a digital Europe happen.

## 2. Guidelines on the Responsible Use and Management of Data

Digitisation is spreading rapidly across all areas of the economy and society. Data is being generated on a large scale and in great variety. Linking and analysing of big data can bring great benefits, but also gives rise to risks which many people see as a cause for concern.

ZVEI and FIEEC are taking these concerns very serious. A priority task of government and business is to create trust in the digital world. It is imperative that this trust will be maintained, because confidence in the responsible use of data is the basis for the emergence of new, data-driven services and business models. Growing interconnectedness is leading to new business models within industries as well. These models are based on the exchange of sensitive data in a value creation network, data which concerns companies' proprietary knowledge and expertise. Confidence in the responsible handling of data is the prerequisite here. ZVEI and FIEEC are entirely aware of this trust building challenge. The companies of the German electrical industry and the French electrical, electronic and digital industries strongly advocate responsible data protection and a safe and secure data infrastructure. Therefore, both associations support a legal framework which allows data-driven business models to emerge in our countries and generate trust in new technologies. Both associations are committed to the essential principal of digital self-determination. We support all efforts which are empowering a secure and safe data infrastructure regardless of personal or non-personal data transaction.

The collection and processing of personal data for new business models must be handled responsibly. The companies of the French and German electrical, electronic and digital industries therefore advocate prudent and careful use of personal data and industrial data for corporate purposes and, to this end, will develop examples of best practice. The electrical industry sees this as an opportunity to develop a common culture of the use of data which is guided by clear values and should not only apply to the European level but also on a global scale. Such a commitment to data related values will enhance competitiveness and will generate a trusted digital environment

### *Commitment to Digital Self-Determination*

The French and German electrical, electronic and digital industries make an explicit commitment to digital self- determination. Digital self-determination is based on the principle of transparency and defines the full capability of controlling self-generated data along the entire data lifecycle.

### *Dialogue as the Necessary Approach to Finding Solutions*

New, data-driven products and services are customized to meet the individual needs of people and companies. They make day-to-day life easier and bring tailored benefits to the customer. At the same time, however, the fear of abuse remains. ZVEI and FIEEC aim to address these concerns through an active dialogue. As new issues in the use of data arise, for example linking or anonymizing data, ZVEI will engage in an active dialogue in order to create a common understanding. In France, FIEEC has a strong cooperation with the French data protection authority (CNIL) in order to define together the recommendations concerning the protection of personal data. One conformity pack has already been published on "smart grids and personal data" and a new one in under development concerning "Silver economy and personal data".

***Rejection of a Monopoly on Technical Data***

Our organizations reject a monopoly on technical data. Digitisation should be designed to allow data to be shared without any blanket transfer, analysis or selective visibility of such data being required. Framework conditions of this kind would force customer relationships into rigid channels and would make both market entry and innovation harder. Flexible formation of customer relationships – throughout the value creation network – will play a decisive role in determining the economic order in the future. It is thus very important to launch a debate on the free and fair use of data and how to guarantee flexibility in customer relationships. In this respect the free flow of data is of utmost importance, in order to raise the potential of the digital economy. Data portability has to be assured with respect of innovation in a European framework.

## 3. Guidelines for a European Cybersecurity Concept

Cybersecurity is not only a basic need to help building trust in the digital world but also a prerequisite of the entire digital transformation of our industries. It is the ultimate objective of a European Cybersecurity Architecture to guarantee a safe and secure communication network both for the consumer and business side.

Building up trust on both the consumer and business side requires a competitive and high quality market of cybersecurity products and services. Our companies require specific cybersecurity design products and concepts that apply not only to B2C or B2B but also to device-to-device connection. In the near future, factories, any kind of devices or products, complex constructions or even entire value chains will be connected. The more virtual interfaces will be connected the higher will be the risk for security. The threat of cross-border cyberattacks, spying and manipulation by states, criminal networks of terrorists or individuals is constantly growing and needs to get the full attention of the political level. It should be of high concern for our governments to protect citizens from attacks against critical infrastructure such as energy, water, transport systems, healthcare etc. On the industry side, cybersecurity needs to apply to any device or virtual gateway. This asks for a bottom up approach of cybersecurity innovation, which can be defined as industrial security encompassing the shop and the office floor. Industrial security means security-by-design which has to be installed on hard- and software. We support the concept of giving identification and security trusted labels to every single device within complex or interconnected systems and processes. FIEEC and ZVEI are appreciating the creation of the cybersecurity PPP which will further develop the field of B2B cybersecurity towards a European approach.

***Strengthening Networking on Security-Related Issues***

Today, the companies of the electrical, electronic and digital industries are already interconnected with their customers, suppliers and employees. In the interest of promoting data security, ZVEI fosters an intensive exchange of information on security-related issues through discussion platforms based on mutual trust, cooperation on the development of guidelines, and the involvement of experts from government agencies. The goal is to establish an ongoing exchange of information between manufacturers, integrators and operators. In France, FIEEC works closely with public authorities, especially the National Agency for the Security of Information Systems (ANSSI) and the Committee for the Security sector (COFIS) to promote cybersecurity.

***Willingness to invest to ensure a culture of security***

Given the importance of data protection and security, companies must be willing to make long-term investments in measures needed to ensure it. Our organizations therefore call for their members to establish a culture of security that starts with senior management. The prerequisites for this are:

- making information security a top-level priority,
- implementing and evaluating risk-based, staged solutions (both in terms of technology and in organizational terms) on an ongoing basis,
- sharing information, for example in the framework of the government initiative "Alliance for Cyber Security" ("Allianz für Cybersicherheit").

***Cooperation on security incidents***

Cooperation between companies and government agencies on a basis of mutual trust makes a valuable contribution toward strengthening risk awareness and data security. This applies in particular to situations in which security incidents have already occurred. ZVEI and FIEEC will strive to heighten this awareness in the electrical, electronic and digital industry.

## 4. Standardisation

The breath-taking pace of advanced technologies perpetually penetrating our economy and society will require flexible and on time applied standards of best performance. FIEEC and ZVEI agreed that norms and standards are of high importance with respect to the digitisation of industry. The EU Commission's priorities on ICT standardisation is a good starting point to further develop the dialogue with our industry as they are developing standards along their products, processes, services and new business models. This is the place where standards have to be developed in cooperation with industrial internet standardisation fora. Members of FIEEC and ZVEI need industry-driven, open as well as bottom-up standardisation procedures. Standardisation should be constituted like a public-private-partnership between the economy and the public authority. FIEEC and ZVEI take the risk very serious that consortia standardisation setting could risk needed coherence of the standardisation system as a whole. Standardisation should always address the international market competition, with a completing, pro-active and constructive procedural management between law making and standardisation appears to be necessary. The digitisation of our economy and society equally requires a radical digitisation of standardisation. Standard-to-machine approaches and the wide connection and acceleration of processes have to stand in focus of the standardisation procedures. Pro-active standardisation could help to catch trends in time and react more flexible. We do not need cemented catalogues of standards but an open development in line with the global market environment. A reduction of complexity of standards will also lead to a reduction of time consuming standards processes. Law making is providing the basic demands, but standards are providing precise definition. The European Single Market is not the ultimate achievement of standardisation, but a starting point to address international standardisation settings.

***

*FIEEC and ZVEI will continue to work together on all dimensions of the digitalisation of our society and economy. Both associations are committed to the Digital Single Market strategy of the European Union and take their responsibility as strong partners respectively this revolutionary and challenging process.*