TÜV®

Author
VdTÜV-WG Cybersecurity

Date
October, 3RD 2015

VdTÜV Statement on the Communication from the EU Commission "A Digital Single Market Strategy for Europe"

VdTÜV e.V. welcomes the Communication on a Digital Single Market Strategy for Europe (COM(2015) 192) presented by the EU Commission. The Strategy has a very important impact on the economic position of Europe and its competitiveness. A unified and balanced digital single European market is necessary in order to overcome the current fragmentation, avoid unnecessary costs and achieve synergies between the activities of the different EU member states.

On the following pages, VdTÜV e.V. will present its points of view regarding the strategy for a digital single market. The Communication of the EU Commission provides vital cornerstones in the field of consumer protection, although VdTÜV considers that some economic aspects should be added to support achievement of a functioning digital single market. The focus will be on cybersecurity, cloud computing, standardisation and interoperability as well as on training. Moreover, cybersecurity in a digitally-networked world must be considered in close cooperation with other regions, such as East Asia and North America.

In the end, concrete implementation of the Digital Union within a solid legal framework will be decisive for its success.

Key messages of the VdTÜV's statement

- Independent, qualified audits by competent bodies provide decisive impetus and stimulus for effective improvement of the IT security architecture of the operator or enterprise.

- An EU-wide framework for certifications according to international standards in the area of information security contributes significantly to ensuring the digital sovereignty of the EU.

- A European cloud initiative should set clear requirements for the security and quality as well as the legal framework of cloud computing.

- Security must be integrated into standards in such a way that in future it is understood as a fundamental performance characteristic of the development and utilisation process (safety & security by design).

- Vocational training and further training must become an integral part of a digital working world and of personnel development. Only raising user-awareness of security measures, along with a basic knowledge of cybersecurity, can ensure sustainable information security at a high level.

1. VdTÜV Statement on Clause 3.4. of the Communication: "Reinforcing trust and security in digital services and in the handling of personal data"

The Network and Information Security Directive (NIS-Directive) is an important step towards strengthening the level of cybersecurity in the EU. IT security that creates trust in critical infrastructures is a decisive factor for the development of digital business. During the forthcoming NIS Directive negotiations, legislators must set concrete requirements and provide transparent rules for execution of security audits in the case of critical infrastructures. In our view, above all the independence and competence of the Bodies entrusted with the execution of security audits must be ensured in the Directive, in order to guarantee that the audit is meaningful and reliable. Audits by independent bodies also mean that enterprises do not have to build up testing competence in-house. **In addition, independent, qualified testing provides decisive impetus and stimulus for effective improvement of the IT security architecture of the operator or enterprise.** By analogy with the Decision on a common framework for the marketing of products (768/2008/EC), we basically endorse use of independent and competent bodies in security audits for high-risk areas in the digital single market.

In addition, we consider it appropriate to create **an EU-wide framework for certifications** according to international standards in the area of information security. Efficient approval and certification processes for IT security products can also contribute significantly to ensuring the digital sovereignty of the EU - in other words security of data communication - without the risk of shutting off from global markets and Internet infrastructures.

We take a positive view of the establishment of a **public-private partnership for cybersecurity** in the area of online network security technologies and solutions in order to drive forward investment in digital transformation. **However, there is no clear statement regarding the planned orientation and objective of the public-private partnership for cybersecurity.** We consider that this partnership should be open to a wide variety of competent partners from industry, above all also from small and medium-sized enterprises and the industry services sector. Tried-and-tested EU funding programs such as Horizon2020, COSME and EFSI and also the "Juncker-Plan" can be used together, in order to create synergies and ensure a practice-orientated focus for the public-private partnership.

We also miss reference to the protection of **non-personal data**, which in the case of networked objects and machines within the "Internet of Things" are mostly generated automatically by means of sensors. These so called machine data are significant for the digital transformation process in general and, naturally, for commercial applications. Machine data are up to now not protected under either civil or copyright law and cannot be clearly allocated to any person with regard to exclusive use or further exploitation. **Legal uncertainties as well as unsettled questions in the areas of interoperability and standardization are damaging to the development of new, data-based markets.**

2. VdTÜV Statement on Clause 4.1. of the Communication: "Building a data economy"

VdTÜV e.V. welcomes the announcement of the EU Commission on **a European Cloud Initiative.**

We agree with the opinion of the EU that above all lacks of trust in security prevent many enterprises from transferring their data to a cloud. The development of trustworthy and secure cloud services in the EU will create a real locational advantage. **In the view of VdTÜV e.V. a European cloud initiative should therefore set clear requirements for the security and quality as well as the legal framework of cloud computing.** These requirements should be considered within a corresponding internationally-agreed standardisation strategy.

Experience in practice has shown that independent and professional certifications in accordance with internationally-recognised standards are a decisive guide for users when it comes to judging the quality and trustworthiness of a cloud service, its provider and all downstream processes such as security, infrastructure, availability etc.

Important security and quality requirements for a cloud service, which should also be contractually fixed between provider and user, include the locality and separation of data, network security and access controls. Data must be stored in encrypted form, in order to prevent subsequent personalisation of data within a cloud in shared or common use. In this connection, the cloud services should be subject to competent certification by an independent body with regard to the criteria of process and structural organisation, data security and compliance/data protection, including legally-compliant data erasure following the end of the contract. Other important criteria include data portability and the user friendliness of the Cloud. In this way, the cloud client can receive a reliable statement regarding the quality, performance and security of the cloud, and the cloud provider has the opportunity to present a positive profile within the competitive environment.

3. VdTÜV Statement on Clause 4.2. of the Communication: "Boosting competitiveness through interoperability and standardisation"

International standards play a decisive role within digitally-networked production, future means of transportation, the Smart Home and also health provision. Many products can only become fit for the market if they can be smoothly integrated into worldwide information and communication networks. Therefore, in the view of VdTÜV e.V., the approach based on European standardisation, as proposed in the Digital Single Market Strategy for Europe, can only be the first step. **European standardisation must always be seen from the perspective and within the context of the international standardisation work and activities of other regions within the global market.**

Among other things, standards promote business interpenetration within the European internal market and help with the development of new and improved products. They are essen-

tial for free and fair global trade. Those enterprises which integrate their know-how with regard to new technologies and the necessary framework conditions into new standards at an early stage can improve their competitiveness and ability to innovate in global markets.

The EU Commission can assume a more proactive role and name standards which it considers to be missing but which would support digitisation of industrial and service sectors. The basis for mandating a European standardisation organisation to draft a standard is Regulation (EU) No. 1025/2012 on European standardisation. It would be useful to refer to national recommendations and existing standardisation roadmaps of the EU member states for industry-specific standards, and also to the expected elaborations of European initiatives, such as the "Alliance for Internet of Things Innovations" launched in March 2015. In addition, existing standards - in particular international standards and global industrial standards - can be included into the European set of standards. In the area of cybersecurity, IT security management systems and cryptoalgorithms play a central role for both Office IT applications and in-process and factory automation. **Security must be integrated into standards in such a way that in future it is understood as a fundamental performance characteristic of the development and utilisation process (safety & security by design).**

In our view, the EU Commission rightly pleads in favour of granting priority to the processes of discussion and agreement with all stakeholders in the standardisation committees over de facto standards or internal standards of international enterprises. Taking due account of ever shorter innovation cycles in the area of digitally-networked technologies and applications presents a challenge when standards are developed within the relevant committees, and there is also the need to create standards with direct market relevance. To counteract this, the experts in the standardisation committees should make use of existing possibilities for more flexible ways of working and formats that facilitate accelerated publication of standards. These include, for example, development of technical specifications as a first step towards later consensus-based standards.

In addition, close cooperation between research and business is useful in order to establish examples of applications for digital technologies, products and services which can be strategically supported so that European interests can participate in a concerted exchange with partners from other world markets. The partners from the worlds of business and research should also participate more strongly in the corresponding committees (ISO, IEC, ETSI, IEEE, OASIS, W3C etc.) than has been the case up to now. Europe's politicians and enterprises must put their full weight behind their participation in the global debate on standardisation.

4. VdTÜV Statement of Clause 4.3. of the Communication: "An inclusive e-society"

VdTÜV e.V. believes that greater efforts in the area of education and training are a central prerequisite in order to achieve positive results in the area of digital transformation i.e. to enable employees of all age groups to participate in this transformation through training and qualification. From the perspective of IT security, technical measures alone are not sufficient in order to defend against threats. Human beings must be sustainably equipped to deal with the challenge of cybersecurity. For employees, the following four competences, among others, are of central importance: the readiness to undertake lifelong learning, interdisciplinary thinking and acting, a higher level of IT competence and the ability to enter into permanent communication with machines and networked systems. **Vocational training and further training must become an integral part of a digital working world and of personnel development.** Further training can take place on an individual basis at the workplace, taking the respective needs and existing qualifications into consideration.

Responsibility for questions of education and training lies with the member states, but the EU Commission can still be active at the overall European level and can provide important stimulus. The quality of further training measures should, for example, be defined through performance and requirement profiles that are harmonised throughout Europe, which can then form a basis for independent and periodic certification. This creates confidence in the benefit of the measures before the investment decision is made and also enables meaningful comparison between the different further training measures on offer in the European single market. In addition, the time between drafting of new requirements for qualifications and their integration into the respective further education measures is shortened.

Furthermore, it would be welcomed if the EU Commission were to work towards a Europe-wide citizens' portal for IT security. **Only raising user-awareness of security measures, along with a basic knowledge of cybersecurity, can ensure sustainable information security at a high level.**