

# Position Paper

## Bitkom views on EDPB Guidelines 2/2021 on Virtual Voice Assistants

23/04/2021

Page 1

### Introduction and Overview

We generally welcome EU-level guidance on voice assistant services that, while guaranteeing adequate privacy protection for users, remains sufficiently open and flexible, so that it can take into account the peculiarities of the different voice service architectures and the rapid technological developments in the sector.

Bitkom welcomes the opportunity to comment on the Draft Guideline. We believe that more cooperation and exchange between data protection authorities and practitioners is needed to translate the legal text of the GDPR into practice and reduce legal uncertainty.

In our view, the Guidelines should be amended especially regarding the paragraphs related to the use of machine learning, service improvements and the appropriate legal bases (e.g. paragraphs 76, 80, 101, 103). The understanding on product/service improvements (para. 80) seems very narrow, especially seeing that, in practice, distinguishing "contract fulfilment" from "product/service improvements" can be difficult, e.g., when data processing or data analysis is performed with the aim of shortening or simplifying internal processes that essentially serve the (contracted) customer service.

We also think that the explanations regarding the ePrivacy Directive should be reviewed as well. It is not entirely comprehensible why VVAs are considered indiscriminately as "terminal equipment", since it is precisely elements of hardware and software that must interact here (para. 25). It is also really important that it is clear in which cases consent would be required under Article 5(3) ("storage or access to information stored in the terminal device", para. 71) and when a legal basis under Article 6 of the GDPR or consent under Article 9 of the GDPR ("any processing operations of personal data subsequently to the storage or access to information in the

Federal Association  
for Information Technology,  
Telecommunications and  
New Media

**Rebekka Weiß, LL.M.**

Head of Trust & Security  
P +49 30 27576 -161  
r.weiss@bitkom.org

Albrechtstraße 10  
10117 Berlin  
Germany

President  
Achim Berg

CEO  
Dr. Bernhard Rohleder

## Position Paper EDPB Guidelines on Virtual Voice Assistants

Page 2|11

terminal equipment", para. 72) is required. In practice, this differentiation will appear artificial vis-à-vis the customers, as it is ultimately about a uniform application, the VVA.

We also consider the clarification of the role as processor or (joint) controller for the respective data processing to be very important (para. 45), especially since it is conceivable that products and services are "responsive" via VVAs. Further elaborations and examples with different constellations would be helpful.

The requirements for transparency leave some questions open so we suggest including further details, especially in para 49 regarding the specificities of the vocal interface. In our view it seems impractical to inform about the processing of the data via the medium VVA by means of "voice information".

Our position paper details our suggestions for amendments below.

### 1. LEGAL FRAMEWORK

#### *a) GDPR*

The core function of a voice service is to accurately recognize and respond to customers' spoken requests. Users want voice services to perform this function well and for the services to improve over time, including by adding new and desirable features. Since the activities involved in voice services are diversified and complex, it is necessary to rely on different legal bases for the data processing.

We agree with the EDPB that the relevant legal framework for voice services is GDPR (see par. 7, 24 of the draft Guidelines). GDPR indeed offers the necessary flexibility to tailor appropriate privacy-protective practices to the particular data processing at stake, as it articulates several legal bases for the data processing – including contract performance, consent and legitimate interest.

In our view, Art. 6 para. 1 lit. b GDPR especially justifies processing insofar as it is "necessary for the performance of a contract to which the data subject is party [...]", i.e. there must be a direct link between the processing of an individual's data and the necessity to provide a specific contractual service to that person.

In many cases, the processing of personal data for machine learning in virtual assistants is a prerequisite for the achievement of the performance of the contract, i.e., in the context of the original purpose of the contract, even if, in this context, data are further processed for new purposes as part of the learning process. In these cases, ML is used to enable the provision of services to the person whose data are processed. The performance requirement of processing personal data for ML is not determined solely by assessing whether a service can be provided at all or not - rather, it is decisive whether it can be provided in the contractually agreed form and quality. To this end, ML-based contractual services often include a dynamic or proactive element for which the user contracts and which could not be performed without the insights from ML.

## Position Paper EDPB Guidelines on Virtual Voice Assistants

Page 3|11

### b) ePrivacy Directive

The draft Guidelines also indicate that, in addition to GDPR, the ePrivacy Directive applies since such directive “sets a specific standard for all actors who wish to store or access information stored in a terminal equipment of a subscriber or user in the EEA” (par. 24). More specifically, Article 5(3) of the ePrivacy Directive would apply because “current VVAs require access to the voice data stored by the VVA device” (par. 28 of the draft Guidelines).

— We believe this characterization does not have a justification in the letter and scope of Article 5(3) of the ePrivacy Directive.

— Article 5(3) must be read in conjunction with Recital 24 of the ePrivacy Directive. According to Recital 24, the situation that Article 5(3) is deemed to address is where “so-called spyware, web bugs, hidden identifiers and other similar devices can enter the user’s terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user.” The use case that the ePrivacy Directive had in mind is clearly different from that of voice services where a user’s device opens a stream to a cloud-based service that fulfils the user’s request. This activity does not generally implicate the use of spyware, web bugs, hidden identifiers, or other similar devices. As the customer speaks to his or her device, this information is directly sent to the cloud for processing without the voice service provider gaining access to the device, whether through spyware or other means. Moreover, customers are typically informed upfront about how their voice recordings are being used, and they can review what utterances have been recorded and sent to the cloud. This transparent structure is quite the opposite of the use case the provision of Article 5(3) is intending to protect against.

Article 5(3) applies to “the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user”. A cloud-based voice service does not generally require storing information or accessing information in the customer’s device. By design, the streaming of the voice recordings to the cloud typically occurs when the voice command of the user activates the voice service. When this happens, the voice service provider does not “store” voice recordings in the device of the user nor “gains access” to voice recordings stored on the device of the user. The opposite happens: it’s the user that initiates the streaming of the voice recordings to the servers of the voice service provider via the device rather than the voice service provider retrieving that information from the device. In a way, the voice command of the user makes a connection to a server, but this does not mean that the server gains access to the user’s equipment. It is like clicking on a hyperlink of a website, or entering text input into a search engine or other web application: the user makes a connection to the server to receive information without the server gaining any access to the user’s device.

Furthermore, following the logic of the draft Guidelines, Article 5(3) would apply to any digital service that is accessed through a device. However, the European legal framework on data protection does not support this interpretation. First, Article 3 sets the scope of the ePrivacy Directive to comprise “the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.” In accordance with the CJEU, notably in *Google LLC v. Bundesrepublik Deutschland* (C-193/18), the definition of an

‘electronic communication service’ mostly comprises the services provided by internet access providers and operators of the various networks of which the open internet is constituted (C-193/18, § 36). The ePrivacy Directive thus normally only applies to the services that are required to access the internet but not the digital services, such as a voice service, that are provided over the internet. Second, applying Article 5(3) to any digital service that is accessed through a device would unduly limit the scope of the GDPR and extend the scope of the ePrivacy Directive. The GDPR applies to the processing of personal data, including the processing of personal data in connection with digital services. The providers of such services notably need to choose one of the six available lawful bases provided for under Article 6 of the GDPR as appropriate for the processing at hand. If one would apply Article 5(3) of the ePrivacy Directive to all digital services simply because they are accessed through a device, this would limit the available lawful bases for a great proportion of processing activities in today’s society as more and more services are in fact being digitalized. This cannot be the intention of the drafters of the two statutes (see also section 3 below).

#### c) Qualification of VVAs as Terminal Equipment

Pursuant to the draft Guidelines, “VVAs should be considered as “terminal equipment” and the provisions of Article 5(3) ePrivacy Directive apply whenever information in the VVA is stored or accessed” (par. 25 of the draft Guidelines). However, no explanation is given as to why that is the case. We believe that the qualification of a VVA as terminal equipment is incorrect. It is inconsistent with the technical definition of VVA in the Executive Summary as “*a service that understands voice commands and executes them or mediates with other IT systems if needed*” (p. 2, emphasis added) or in par. 8 of the same draft Guidelines as “*software application that provides capabilities for oral dialogue with a user in natural language*”, which clearly refer to a VVA as a service, not an equipment.

The ePrivacy Directive does not define “terminal equipment”. The term is defined in the Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment as “*equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information [...]*.” According to the Merriam-Webster online dictionary, equipment refers to “*the set of articles or physical resources serving to equip a person or thing [...]*.”<sup>1</sup> It is thus clear that the notion of “terminal equipment” necessarily refers to a physical device and does not cover services.

Moreover, Article 5(3) of the ePrivacy Directive refers to “*the terminal equipment of a subscriber or user,*” suggesting that the terminal equipment belongs to the subscriber or user. This can only make sense where the terminal equipment is a physical device. Construing the notion of “terminal equipment” as including voice services clearly stretches the scope of Article 5(3) past the article’s semantic constraints. A service is not something that an individual user would possess as one would possess a physical device. If anyone owns the voice service, it is the provider that

---

<sup>1</sup> <https://www.merriam-webster.com/dictionary/equipment>.

offers that service. Any other interpretation would make GDPR inapplicable any time there is a device involved, which we assume it is not the objective that the Guidelines intended to achieve.

For all the reasons above, we recommend that the EDPB re-considers the references to the ePrivacy Directive contained in the Guidelines in light of GDPR and the EDPB's previous guidance.

#### d) Cooperation and consistency mechanism

The GDPR has introduced the cooperation and consistency mechanism in relation to its provisions (Chapter VII, GDPR), which the EDPB considers applicable even if the processing of personal data in part relies on access to information stored in the end-user's device (see EDPB Opinion 5/2019). The Guidelines should clarify that data protection authorities should apply the cooperation and consistency mechanism provided by the GDPR when applying privacy provisions in the context of voice services.

## 2. QUALIFICATION OF THE VOICE SERVICE PROVIDER

The draft Guidelines provide that “[f]rom a high-level perspective, the designer may act as a data controller when determining the purposes and means of a processing, but may intervene as a processor when processing personal data on behalf of other parties, such as an application developer” (par. 42 of the draft Guidelines). We welcome that the EDPB does not adopt a rigid position on the qualification of the different stakeholders involved in the provision of a voice service. As the EDPB rightfully states, “the applicable qualifications have to be established on a case-by-case analysis” (*id.*).

However, in its illustrative example of a relationship between a voice service provider and a bank offering an application that the customers can query directly via the voice service concerned, the EDPB determines that the voice service provider qualifies as the bank's processor without consideration of other potential qualifications. In fact, a voice service provider may often qualify as an independent controller, with its own independent purposes, when making third-party applications available via its voice service.

For example, when processing the customer's voice input and other associated personal data and transmitting the content of the customer's request to the third-party application concerned, a voice service provider may independently determine both the purpose and the means of the processing. The purpose consists in performing the voice service provider's contract with the customer, that is to say providing a voice service that interprets and responds to the customer's spoken requests. Regarding the means of processing, the voice service provider may also determine which data are collected (*i.e.*, the customer's voice input and other relevant personal data), which data will be transferred (*i.e.*, the relevant content of the customer's request as interpreted by the voice service provider), and to whom (*i.e.*, the appropriate third-party application developer). Finally, the voice service provider may also independently be responsible for complying with its obligations to customers in respect of these processing activities (*e.g.*, informing customers of the processing activities or responding to data subject requests).

This situation can be compared to the example of the travel agency ExploreMore in the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR. ExploreMore arranges travels on request from its individual customers. Within this service, they send the customers' personal data to airlines, hotels and organisations of excursions in order for them to carry out their respective services. Pursuant to the EDPB, *"ExploreMore, the hotels, airlines and excursion providers are each to be seen as controllers for the processing that they carry out within their respective services. There is no controller-processor relation"* (p. 29).

As with the travel agency ExploreMore, the voice service provider arranges voice experiences on request from its individual customers. Within this service, the voice service provider may sometimes send the customers' personal data to third-party applications in order for the developer of these third-party applications to carry out their respective services. Accordingly, each of the voice service provider and the developers of the third-party applications qualify as individual controllers in that situation.

The EDPB should therefore take into account in its banking application example that a voice service provider may also qualify as an independent controller when implementing a third-party application, with the qualification of the different stakeholders ultimately depending on a case-by-case analysis.

### 3. LAWFUL BASES

The draft Guidelines read as though the only available lawful basis for the processing of personal data in the context of a voice service are consent and, in very limited circumstances, contract performance. The EDPB in fact states that, *"[i]f processing is not strictly 'necessary for the performance of a contract' within the meaning of Article 6(1)(b) GDPR, the VVA provider must, in principle, seek the consent of the data subject."* The reason for this would notably stem from the fact that *"reliance on legitimate interest could, in certain cases, risk undermining the additional level of protection provided by Article 5(3) of the e-Privacy directive"* (p. 23 of the draft Guidelines).

Having consent as the only option cannot be the intended effect of applying Article 5(3) of the ePrivacy Directive to the provision of voice services. Other lawful bases, such as "performance of a contract" or "legitimate interest", provide in most instances for a strong, protective and much more appropriate lawful basis. "Performance of a contract" under Article 6(1)(b) GDPR constitutes the appropriate lawful basis (see above), for instance, for service improvement purposes or for certain content personalization purposes, as the EDPB states (par. 85 of the draft Guidelines), because those purposes participate in the fundamental objective of a voice service, namely ensuring that customers can effectively and securely interact with the voice service.

Especially seeing new developments such as machine learning in the context of all voice assistants it is in our view important to take a closer look into necessary data processing in the context of the contractual relationship in question. Machine Learning, f.i., is not entirely new, and for more historically ML-based products and services, its use and necessity in the context of contractual performance requirements has never been questioned. For example, many cars have automatic transmissions that learn the driver's personal preferences and adjust the shift accordingly. In the event of a faulty shift or to improve performance in general, newer vehicles are networked to provide learning data to

## Position Paper EDPB Guidelines on Virtual Voice Assistants

Page 7|11

the manufacturer, and older vehicles, the findings are often read to solve performance problems. The associated processing of personal data is necessary to fulfil a contractual obligation and, is necessary to maintain a defect-free product. There is no repurposing of personal data for ML; rather, the learning enables the service provision, since without the learning process no adaptive automatic transmission could be offered.

The same applies to all other types of contract performance that require ML for proper fulfilment. The need is determined by the agreed performance. For the agreed performance in the assured quality the processing of personal data on ML via voice recognition can therefore be contractually necessary and also justified according to Art. 6 para.1 lit. b GDPR.

This applies, for example, to services such as natural language recognition, which are extremely complex and independent of the development effort in advance and the testing of beta user groups always show a lack of understanding, e.g., for regional peculiarities such as dialects or accents, which the user expects as part of his natural language, but which the system can only learn over time. Under the relevant contracts, users also expect that natural language recognition systems keep pace with language development. This is quite a challenge: new words or phrases become popular or are invented - sometimes overnight. Micro-dialects emerge and adapt. Most language understanding engines rely on machine learning to adapt to changing speech and language patterns in real time. Customers seeking spoken language understanding ("SLU") services expect these services to continue to function and work when speech patterns occur or change. They determine the "natural language" and would be frustrated if they had to wait for a new pattern to be officially recognized by linguists sometimes years later. The provision of SLU services therefore requires a proactive element that only ML can provide. This is precisely what therefore makes the data processing via the voice assistant and the Machine Learning process behind it a contractual requirement.

The pursuance of a legitimate interest can also constitute a valid lawful basis for data processing that is done by voice service providers. The voice service provider, for instance, has a legitimate interest in offering an attractive product that continues to improve and add new features over time, just as the customers have a legitimate interest in receiving new desirable features. With appropriate safeguards in place, such as an unconditional and easily accessible way to opt-out from the processing, Article 6(1)(f) GDPR can indeed be an appropriate lawful basis.

Ruling certain lawful bases out from the outset eventually negates the principle that the appropriate lawful basis must be determined on a case-by-case basis by the data controller. This principle is made really clear in the Article 29 Data Protection Working Party (WP29) guidelines on DPIAs endorsed by the EDPB: *"it is the responsibility of the data controller to assess the risks to the rights and freedoms of data subjects and to identify the measures envisaged to reduce those risks to an acceptable level and to demonstrate compliance with the GDPR"*. Equally, the still applicable WP29 guidelines on legitimate interest provide that: *"In the first place, before a processing operation on the basis of Article 7(f) is to take place, the controller has the responsibility to evaluate whether it has a legitimate interest; whether the*

---

<sup>2</sup> wp248rev.01.

*processing is necessary for that legitimate interest and whether the interest is overridden by the interests and rights of the data subjects in the specific case.”*

The EDPB’s statement on the available lawful bases further suggests that Article 5(3) of the ePrivacy Directive applies to any processing activity in the context of a voice service. However, Article 5(3) only applies to “*the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user.*” A voice service in fact does not necessarily require storing or accessing information in the device of the customer. When a customer utters a voice command, the voice service provider does not retrieve that information from the customer’s device but receives it as part of the customer’s request. This is no different to a customer clicking on a hyperlink of a website as it is the customer who initiates the connection with the server of the website and not the server that gains access to the customer’s device.

In light of the above, we recommend a revision of the EDPB’s statement, as it relies on a wrong assumption and other lawful bases such as the performance of a contract or the pursuance of a legitimate interest under Article 6(1)(f) GDPR may be valid for data processing by voice service providers.

#### **4. SERVICE IMPROVEMENT**

In section 3.4.2 of the Guidelines, the EDPB analyses the appropriate lawful basis when processing personal data to improve the voice service’s performance or to develop new functions within the voice service. More specifically, the EDPB considers the case where the voice service provider transcribes the customer’s voice input and feeds it into the voice service’s training dataset for machine learning purposes. The transcriptions of the customer’s voice input are reviewed and corrected by humans. The EDPB concludes that such processing cannot be based on “performance of a contract” under Article 6(1)(b) GDPR. According to the EDPB, “[t]he main reason being that VVAs are already functional when they come out of the box and can already perform as (strictly) necessary for the performance of the contract.”

We believe this approach overlooks the overlap between maintaining and improving the performance of a voice service and traditional software debugging. Rather, the various types of data processing required to provide, maintain, or improve a voice service should each be independently analysed under Article 6(1)(b) and Article 6(1)(f) GDPR. Taking that approach, either contract performance or legitimate interest can be appropriate justification for the processing of customer data.

Contract performance, in particular, can justify the quality assurance and quality control activities voice service providers engage in to ensure that services meet customer expectations. Contrary to the draft Guidelines, voice services are not always functional “out of the box” or always able to perform as needed or expected by customers. This is precisely illustrated in the example provided in the draft Guidelines where the customer of the voice service has to issue three times the same voice command due to the voice service not understanding it. The substance and fundamental objective of the contract between a voice service provider and its customers consists in ensuring that customers can effectively and securely interact with their voice assistant. To this end, the service must not only

recognize specific speech patterns, vocabulary, dialects and grammatical structures (from proper to slang) in different acoustic environments but also adapt to the diverse and evolving nature of human voice.

Voice services must necessarily learn how to interpret new (and varied pronunciations of) words and phrases that emerge over time. For example, when the assistant Echo was first introduced, customers did not ask Alexa to play songs by artist Lil Nas X. In 2019, he was one of the most requested musicians, and f.i. home voice assistants had to quickly learn all the varied ways customers pronounce his name and request to play his music. This illustrates that an effective voice service cannot stay frozen in time but has to evolve with the humans it interacts with. Similar considerations would apply for terms such as “coronavirus”, “Covid-19” or “practicing social distancing” that were not commonly in use before the Covid-19 pandemic. Maintaining a voice service that is able to correctly understand and respond to customers’ evolving requests is necessary to meet customers’ contractual expectations of how a voice service should perform.

Service improvements targeted at specific dialects, colloquial uses of language, or accommodating users with language impairments further ensure that voice assistants work well for everyone, and are essential to maintaining the quality of services promised to customers.

Service improvements are also crucial in ensuring the security required to maintain the service operational. For instance, accuracy improvements help reducing so-called false wakes, where the voice service starts listening upon erroneously detecting a certain word as a “wake word” selected by the customer. Providing a secure product is clearly part of the fundamental objective of the contract between the customer and the voice service provider. Voice service providers must therefore be able to rely on the performance of the contract under Article 6(1)(b) of the GDPR to learn from so-called false wakes to improve activation accuracy of the voice service and reduce their recurrence.

The EDPB should therefore revise its conclusion regarding service improvement purposes and consider Article 6(1)(b) of GDPR as an appropriate lawful basis.

## **5. VOICE RECOGNITION**

### **a) Voice recognition**

According to the draft Guidelines, the EDPB is of the opinion that voice recognition may only be activated “*at each use at the user’s initiative, and not by a permanent analysis of the voices heard by the assistant.*” The EDPB explains that when the voice service is set to permanently listen for the voice of a registered user, “*the voice of non-registered and accidental users will also be processed for the purpose of uniquely identifying them*” (p. 30).

This is not factually accurate. Users who wish to be recognized when using a voice service generally must train the voice service to recognize the user’s voice. Depending on the provider, they may do so by creating a “voice profile”. A voice profile enables the voice service to recognize a user’s voice, call them by name, and provide enhanced personalization. But it may not enable the voice service to recognize the voices of *other* users who have not created a voice profile. When the voice recognition service analyses an unknown voice making a request (including, possibly, a

voice from a non-registered user or an accidental wake), it does so to determine whether the voice matches a stored profile of a registered customer who gave their consent to use the voice recognition feature. The voice service simply rules these customers out as *not* the registered user. Logically, there is indeed nothing unique about *not* being a specific individual.

Based on this, we encourage the EDPB to revise its recommendation that voice recognition may only be activated at each use at the customer's initiative.

#### b) Voice templates' storage

The draft Guidelines state that “[v]oice templates should be generated, stored and matched exclusively on the local device, not in remote servers” (par. 133). This is inconsistent with the WP29 guidance on biometrics. In that document, the WP29 recognizes that the biometric template of a customer can be stored in several ways, including in a central database. The WP29 confirms that “*identification can only be achieved by storing the reference data in a centralised database, because the system, in order to ascertain the identity of the data subject, must compare his/her templates or raw data (image) with the templates or raw data of all persons whose data are already centrally stored*” (p. 5).

While some of the more basic processing operations can be performed locally in the customer's device, for many voice service providers most of the processing operations that are necessary to effectively provide the voice services, including the matching of voice templates, rely on the more powerful processing capabilities of the cloud.

There are benefits for the users in storing voice templates in the cloud because they can be recognized and receive the same personalized experience when interacting with multiple voice service endpoints linked to their account, and even on devices that do not have sufficient storage and/or processing power to perform on-device voice identification.

From a security standpoint, if the voice template is stored in the cloud, any potential security issues with the devices cannot compromise the security of the voice templates. If a device is stolen or it changes ownership, there is no risk to expose biometric data stored on the device. Storage in the cloud prevents the unauthorised reading, copying, modification or removal of biometric data should one of those events occur.

Storage of the voice templates in the cloud also has advantages because the biometric data is protected by the security controls of the voice service provider that is typically able to apply security updates and patches in the cloud rather than having updates pushed out to all of the devices (or relying on third-party manufacturers to push out updates). This allows service providers to react more quickly to potential new vulnerabilities and does not gate the updates based on device capabilities.

---

<sup>3</sup> [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf).

**Position Paper**  
**EDPB Guidelines on Virtual Voice Assistants**

Page 11|11

Given the longstanding WP29 guidance, the current technical capability and the advantages of storing voice templates in the cloud as described above, the EDPB's recommendation should not be limited to local storage and processing but also consider cloud processing and storage of the voice templates. With the necessary security measures in place to protect the personal data of the customer, cloud processing is indeed an appropriate alternative to local processing.

\*\*\* \* \*\*\*

While we hope that the EDPB will consider our recommendations in drafting its final guidance, we would ask that, at a minimum, the EDPB recognise that the Guidelines will require significant work to implement and recommend to its members to delay enforcement for at least six months after the finalisation of the Guidelines, so as to provide stakeholders a sufficient period for implementation and contractual changes recommended by the Guidelines.

Bitkom represents more than 2,700 companies of the digital economy, including 2,000 direct members. Through IT- and communication services alone, our members generate a domestic annual turnover of 190 billion Euros, including 50 billion Euros in exports. The members of Bitkom employ more than 2 million people in Germany. Among these members are 1,000 small and medium-sized businesses, over 500 startups and almost all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the digital media sector or are in other ways affiliated with the digital economy. 80 percent of the members' headquarters are located in Germany with an additional 8 percent both in the EU and the USA, as well as 4 percent in other regions of the world. Bitkom promotes the digital transformation of the German economy, as well as of German society at large, enabling citizens to benefit from digitalisation. A strong European digital policy and a fully integrated digital single market are at the heart of Bitkom's concerns, as well as establishing Germany as a key driver of digital change in Europe and globally.