Sector Inquiry – Messenger and Video Services

Summary

Central question of the inquiry

Messenger and video services have become an indispensable part of day-to-day communication for many. Consumers can exchange text and voice messages as well as data and make (video) phone calls on different devices. All these features can be used individually and in combination with one another, giving tried-and-tested ways of communication a modern design. Consumers' **requests for individuality or tailor-made solutions** to suit their individual needs translate into a large **variety of business models and applications** in the area of messenger and video services. The Bundeskartellamt has already published an interim report to this sector inquiry in which it explains that the features, offers and economic significance of messenger and video services vary considerably. Besides services which are particularly well known by the greater public, there is a large variety of players ranging from international services run by large corporations, which have millions of users, high turnover numbers and their own digital ecosystems[1] and also hold strong positions on adjacent markets, to services focussing exclusively on Germany or German-speaking countries or services with a focus on special businesses as well as open-source services or free non-profit

---

[1] The term "digital ecosystem" refers to a number of services provided by a corporation mutually affecting one another, see also *Bundeskartellamt*, Stellungnahme zur öffentlichen Anhörung des Wirtschaftsausschusses zum Digital Markets Act (available in German only), 25 April 2022, available at: https://www.bundestag.de/resource/blob/891308/f13edcf322cc218da602e6dc4b58391b/ADrs-20-9-59_Stellungnahme-Mundt-data.pdf and *Bundeskartellamt*, The Evolving Concept of Market Power in the Digital Economy – Note by Germany, available at: https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/OECD_2022_Competition_Committee_Concept_Market_Power_Digital_Economy.pdf?__blob=publicationFile&v=2. See for example also *Fletcher*, Digital competition policy: Are ecosystems different?, Note for the OECD Hearing on Competition Economics of Digital Ecosystems, available at: https://one.oecd.org/document/DAF/COMP/WD(2020)96/en/pdf In information technology the term "ecosystem" refers to software and hardware architecture which is based on proprietary devices, systems and access conditions and thus requires and produces corresponding accessories, see the German-language *Wikipedia* article on "Ecosystems", available at: https://de.wikipedia.org/wiki/%C3%96kosystem.

applications. The industry is active worldwide and generates technological and digital developments and innovation, not just by major players. Competing services stand out by implementing innovative business models and specialising on particular services and features. Independence and protection of personal user data is a major field of expertise and commitment, not just in the area of free systems and applications. However, the general state of the market gives reason to assume that this potential has not yet been fully tapped, spread across all areas of the market and applied in a way to achieve the high level of data protection that would be conceivable. This situation has given rise to new **issues in the area of consumer rights**. Consumers themselves, however, do not seem to prioritise these consumer rights aspects over other criteria when selecting their messenger or video service. For this reason, the central question of this final report on the sector inquiry into messenger and video services is how to promote **data protection as a competition parameter** to achieve better data protection in all messenger and video services on the market. What incentives and measures are necessary for consumers to select their messenger and video service also based on aspects of data protection? And how can providers of messenger and video services be motivated to use data protection to differentiate themselves from their competitors and provide better and more information on this aspect to consumers?

The Bundeskartellamt started its inquiry by looking into the initial situation regarding data security and data protection and the competitive environment in the industry. It focussed on the technical basics and methods of messaging and exchanging audio and video files. The technical conditions and practices of the individual services do not only impact **data security and the (lawful) implementation of data protection measures**. The technical infrastructure can also influence competitive processes, which is why it is key to the Bundeskartellamt's goal of promoting data protection as a competition parameter. It determines, for example, if and to what extent it is possible to access and connect with other messenger or video systems or to integrate technical innovations into a system. The complexity of the technical infrastructure and procedures is also likely to affect the consumers' initiative. Consumers will only be willing to use data protection as a selection criterion as described above if they are able to understand the basics of the complex technical contexts. Any recommendations for action must be based on the **consumers' perspective.** Consumers and services must be motivated to attach a higher priority to data protection in competition through the right conditions and incentives. The Bundeskartellamt surveyed over 40 different services on these matters and conducted a number of expert talks. The authority also assessed a number of studies and technical articles.

Procedure and other issues

In its **interim report** published in November 2021, the Bundeskartellamt presented its investigation results regarding two of the subject matters it investigated: On the one hand, the authority gave an overview of the conditions in the **sector** and the various groups of providers, functions and business

models. On the other hand, it presented initial results of the company survey on **interoperability**. The interim report dealt with the question of whether such interoperability would influence data security and hence the level of data protection in messenger and video services and to what extent interoperability is expected to affect incentives for innovation and the intensity of competition in the sector.

In this **final report** the Bundeskartellamt added its findings regarding data protection in messenger and video services, especially in terms of **data security and data processing**, to the aforementioned considerations. The investigation results are presented, put in perspective and reviewed under legal aspects. Furthermore, the investigation results on **interoperability**, which had not yet been available when the interim report was published and refer in particular to the technical implementation and design, are presented and put into relation to the corresponding stipulations of the **Digital Markets Act (DMA)**, which has meanwhile entered into force, namely on 1 November 2022. Against this background, **approaches for more data protection through competition** are developed which refer both to consumers and the services. The report concludes with **recommendations for action** to improve the level of data protection in messenger and video services in Germany, addressing the legal requirements and the practices regarding tender procedures and public funding as well as the public sector's function as a role model. Decision-makers are encouraged to improve the **conditions for data protection through competition** and introduce a transparent scheme to assess the quality of data protection.

Criteria for data security and data protection in messenger and video services

For this sector inquiry the Bundeskartellamt looked into the technical basics of messaging and audio/video exchange in great detail. The authority has created a **checklist** of essential criteria for data security and data protection. The first item is the **protocol** including state-of-the-art end-to-end encryption. The protocol can be regarded as the language used by a messaging or video system which comprises the rules for exchanging data and connecting to the system. **End-to-end encryption** ensures that the data exchanged between the sender and the receiver cannot be read by anyone other than the communicating parties. Encryption only makes sense if the users exchanging encrypted data are uniquely identifiable. Using **two-factor-authentication** consumers can safely identify themselves to their messenger or video service and their communication partners.

If services generally apply **international technical standards**, the quality level of their technical setup can be considered to be tried-and-tested to some extent. Another advantage of such standards is that it is easier to establish interoperability if communication is based on identical technical principles. Expert third parties can review the system's data security if the **source code of a messenger and video service is accessible**. If this is not the case, there should be a possibility to carry out security audits by independent and renowned auditors and the results should be published. For

users who do not read the privacy statement, the type of business model can be an indicator of whether or not data are used for other unknown purposes. In the event the business model is suspicious, users should make sure to **limit the amount of data they share to a minimum**. If users have to create an **account** to use a service, as is the case with services provided by large corporations which operate their own digital ecosystem, they already provide a lot of data in this process.
For a lawful implementation of data security, messenger and video services must physically store the data of EU citizens **within the area of application of the GDPR** and not transfer them to other jurisdictions. In particular, data must not be stored in the USA, where intelligence services can access the consumer data stored in this jurisdiction. Consumers can protect their own data and those of their contacts by **rejecting contact synchronisation** or by selecting or instructing their service accordingly.
The investigation results had to be assessed based on several criteria. First, it had to be checked whether the technology used for data security and data protection corresponds to the **latest standards** and is viable in the long run. This aspect gained importance against the backdrop of the potential interoperability of messenger and video services and its effects on data protection and data security. In November 2022, shortly before the sector inquiry was concluded, the DMA entered into force. It contains an **interoperability regime** for gatekeepers and has thus made the legal situation regarding this matter more specific. And finally, the **consumers' perspective** also had to be considered. Clear conclusions on whether consumers are willing and able to inform themselves about complex technical matters and make choices in favour of better data protection could not be reached through several consumer surveys and scientific examinations. It is also not clear whether and to what extent the **information on and presentation of data protection facts** by the services is suitable to actually "get the message across" to consumers. There are doubts in light of the present state of the market and the continuously strong position of well-known services.
The investigations have shown that the messenger and video services sector has a lot of **innovative power and expertise** when it comes to independence and the protection of personal user data. However, the sector also applies **a number of inadequate practices**. The results of the sector inquiry give reason to believe that several of the services are not fully committed to data protection issues and do not apply their expertise or implement the possibilities they have to provide a level of data protection that would be desirable from the users' perspective. It is, however, difficult to verify these assumptions based on individual groups of services. While free messaging systems and open-source services showed good results for a number of the criteria, the question of how data security is implemented in detail ultimately depends on the selected (server) operator. Generally speaking, users have **a number of options** requiring a certain awareness of security-relevant behaviour, e.g., as mentioned above, when it comes to **selecting the server operator** or activating **end-to-end**

encryption. Conversely, consumers willing to find such information have **a wide variety of options** to select data protection settings in their messenger or find the client which best meets their requirements and is also viable in the long run because it does not process an excessive amount of data and uses international standards.

Some video conferencing services also offer their users many options, which is often due to them focusing on the requirements of their business customers. They are able to implement a high level of security. Ultimately, however, the respective **host or administrator is responsible** for acting in a security-conscious manner, regardless of whether they act in a business or private context.

Inadequate practices and the lack of commitment become evident for example when it comes to **encryption.** Some popular messenger and video services surprisingly **do not use the latest technology** and only apply transport encryption, for example, or use end-to-end encryption only for certain functions although there is no technical restriction to justify this. It would be desirable to see further security procedures like data encryption on the terminal device, storage encryption, two-factor authentication and backups implemented more frequently in the sector. Another aspect is the legal analysis. Some services either **store data from European users outside the area of application of the GDPR**, which is unlawful, or the precise storage location remains unknown. Various services also process third-party data when **synchronising the contact list**, which can be inadmissible.

Legal assessment

In a first step, the Bundeskartellamt requested information on data storage, data transfer and the synchronisation of the contact list from the messenger and video services and analysed the findings from a legal point of view. The investigation results suggest that some messenger and video services may be **in violation** of the provisions set out in the GDPR.

Synchronising the contact list results in the contact details of non-users also being collected. In the Bundeskartellamt's current view, this common practice adopted by many known messenger and video services is not compliant with the requirements under Article 6(1)(a) GDPR if it is employed on a permanent basis. The data still contain references to persons even if the telephone number is replaced by a cryptographic hash value linked to the user from whose contact list the telephone number was obtained. The purpose of protecting legitimate interests does not further legitimise the controller's processing since the benefit of linking data seems to be too small.

The findings on how data are processed suggest that some messenger and video services are not in compliance with the law when **transferring data to third countries or storing data on servers located in third countries** (Article 45 GDPR). This especially applies to those services which store data of users in Germany in the USA. Personal data may be transferred to countries outside the EU and the European Economic Area only if an adequate level of protection is ensured in the relevant third country (Article 45 GDPR). However, the previous EU-US Privacy Shield negotiated between the EU

and the USA has become invalid following the "*Schrems II*" judgment handed down by the Court of Justice of the European Union in summer 2020.

In addition to possible violations of the GDPR, the authority also legally assessed whether consumers are possibly mislead by the **omission of information** (Section 5a(1) of the German Act against Unfair Competition (UWG)) **with regard to end-to-end encryption**. In the Bundeskartellamt's view, it may not be easy to substantiate a violation of transparency based on the omission of information regarding the type of encryption. For a possible violation of the transparency requirement set out in the UWG the "commercial relevance" of security features, such as end-to-end encryption, would have to be substantiated. However, the market has developed since the planning of the sector inquiry. End-to-end encryption has become the established standard in the industry so that with regard to this security feature it should not make a difference with which service users register. Against this backdrop, it was surprising that some known services do not implement end-to-end encryption or do so only to a limited extent. In order to better assess the consumers' perspective, further inquiries, such as conducting a consumer survey, would have been necessary; however, due to the complexity of the notions in question, the chances of further clarifying the matter would have been uncertain. The question of how to classify the consumers' conduct from the companies' perspective also remained unclear since the messenger and video services provide numerous free offers. Ultimately, it was not possible to provide a final assessment and the matter has to be **clarified in each individual case**.

Interoperability

Since the Digital Markets Act entered into force in November 2022, the legal situation of messenger and video services has been clearly specified with regard to interoperability. Due to the continuing legal policy debate on the statutory obligation for messenger and video services to allow interoperability, the Bundeskartellamt had already asked the companies surveyed in the context of its sector inquiry questions regarding this set of issues **before an agreement was reached in the trilogue on the DMA in March 2022**. As already outlined in detail in the interim report, the Bundeskartellamt's company survey had a clear focus. The aim was to follow up on the expectations expressed several times that interoperability would make it easier to switch to privacy-friendly messenger services and thus improve the **quality of data protection** in this sector. Other objectives associated with interoperability, such as ensuring connectivity in interpersonal communication or reducing the market power of leading messenger services, were not directly covered by the inquiry. According to the results outlined in the interim report, the technical requirements, the data security architecture, the mutual effects of interoperability on incentives for innovation and the intensity of competition as well as consumer behaviour could be seen as the main **factors influencing** privacy effects based on interoperability. Overall, the survey showed that the relevant companies do not

flatly reject interoperability. On the contrary, interoperability or at least forms of exchange are already implemented in some areas to a varying technical depth and scope. Standardisation committees are developing the technical basis for interoperability in a global context. However, this information was accompanied by the clear position held by a large part of the industry that a statutory obligation to allow interoperability across the sector would do more harm than good and should therefore be rejected. Companies taking a rejecting stance particularly fear that forced interoperability would have negative effects on innovation activities and thus also on the level of data security and data protection in messaging and video-conferencing.

The Bundeskartellamt had identified that the findings from the industry survey verify how diverse and complex it is to **analyse the causal relations regarding the issue of interoperability**. When implementing interoperability, not only the investments necessary to technically change the services or develop technical innovations should be taken into account. Possible positive or negative welfare effects caused by changed incentives for innovation and effects on business strategies and the intensity of competition would also have to be considered.

According to the **concept of an interoperability obligation as provided for under Article 7 DMA** only the messenger services that have been designated as gatekeepers are subject to this obligation. In addition, this obligation only becomes effective once another service (voluntarily) approaches the gatekeeper with a corresponding petition. Lastly, merely the basic functions are covered by the obligation. Nevertheless, the practical challenges associated with this are likely to be substantial.

Data security must be ensured in technical terms also when implementing interoperability. Due to the many individual solutions provided by the services and the technical challenges posed by interoperability a **market-wide interoperable end-to-end encryption** is still a challenging issue. In addition, numerous data-related difficulties have to be overcome. This concerns, for example, **data monitoring and data management issues**, which arise when data are passed through several hands. If various services deal with contact lists and data storage in different ways, it has to be ensured that their **conduct complies with the law at all times**. Whether and to what extent **opportunities for innovation** can be maintained is a complex question which cannot be solved on a theoretical basis. The findings of the investigation have shown that this is certainly open to doubt. It is true that the DMA's interoperability regime is limited to the services' basic functions. However, the services' architecture and the technical arrangement of the individual functions in the context of this architecture are very unique so that interoperability would require standardisation and adjustments to varying degrees, which could also affect the forces of innovation in various ways.

Ultimately, the assessment depends on the development scenario assumed in this context. If only individual or a few **bilateral agreements** were to be reached between gatekeepers and petitioners, the challenges would appear to be surmountable, especially since the petitioners voluntarily accept

the difficulties. A large number of individual reference offers, however, seems to be a disadvantage from an economic perspective, which is why corresponding market-wide standardisation would then have to be discussed. Based on the Bundeskartellamt's investigation results, the latter does not seem very likely at this point in time. It cannot be ruled out that the interoperability obligation for gatekeepers **creates opportunities for newcomers** who depend on having access to the large networks of leading services.

Approaches for more data protection through competition

The quality of data protection does not seem to receive the necessary attention within competitive selection processes, especially from users in their capacity as consumers and also from some services. It is therefore unlikely that the level of data protection will improve in a market-driven way under the currently given framework conditions. Instead, privacy-friendly services must be strengthened in competition. It also has to be examined which incentives are necessary for customers to recognise the quality of data protection as an essential product feature and switch to privacy-friendly services.

Competitors of established services pointed out **discriminatory tender specifications** for messaging and video services creating objectively unnecessary obstacles. In this regard, it would have to be assessed which specifications are in fact necessary to fulfil the desired function. A less restrictive attitude towards additional specifications, regarding size and turnover for example, could possibly pave the way for privacy-friendly services.

Many of the services surveyed expect a review of the current **practice of funding open source products and standardisation** to have positive effects on the level of data protection. The entire software life cycle should be included in this context for the benefit of the users' data security. Not only the newly developed application or innovative technology but also the continuous maintenance and management of the products established in the market on this basis and used by consumers seems worthy of being funded in order to achieve data security.

If, in addition, the public sector were to increase the use of privacy-friendly services, this would send out a positive signal for data protection. However, the Bundeskartellamt's findings suggest that there may still be room for improvement. Privacy-friendly messenger and video services have so far clearly not been able to prevail over widely used services – neither in terms of being selected nor in terms of being used against payment in the public sector. Industry representatives also provided numerous examples of how much effort and persuasion is needed for privacy-friendly messenger and video services which are less well-known than the established services to be taken into consideration. This particularly applies in areas where many consumers are to be reached, e.g. in public service

broadcasting, but also in cities and municipalities, federal ministries, administrative bodies and in the educational sector.

With regard to **data protection as a quality feature**, it has not become evident that many consumers choose their messenger and video services based on the fact that they are privacy friendly. If they do try to select a service based on this criterion, users have to deal with a great imbalance of information in favour of the services and to their disadvantage. Consumers would first have to find out which information is relevant in the first place, then search for this information and develop a basic understanding of the matter before finally forming an overall opinion based on several criteria and comparing the services available. In a **technology-based industry**, there seem to be insurmountable obstacles: The technical criteria, procedures and practices which determine the quality of data protection of a messenger and video service are complex and difficult to understand for lay people. As a result, the messenger and video services hardly feel any pressure, at least outside the business customer segment, to enable consumers to make an informed decision with regard to data protection.

In the course of current developments, further challenges are emerging: The DMA's rules on interoperability will pose further challenges for data security and therefore data protection. The services are set up differently in technical terms. Many well-known services have been designed as closed systems. The users' data may therefore be exposed to new risks. This requires great attention if interoperability is implemented. At the same time, however, the information available can become even less transparent for consumers.

*The **complexity of the information needed can be illustrated based on the example of encryption**, even if for the purpose of simplicity greater technical details and complex technical terms are omitted. First of all, different **versions** of encryption have to be distinguished. Transport encryption means that the channel through which a message is transported is encrypted. The message, however, can be viewed by both the users of the messenger and video service themselves and the operator of the server. Unlike transport encryption, end-to-end encryption ("E2E encryption") involves sending the message in an encrypted form across all transmission stations. Only the communication partners at the respective ends of the communication can decrypt the data. Both versions can each be used individually or in combination. In the latter case, the level of security offered is the highest. **Various cryptographic techniques**, such as symmetric or asymmetric encryption with public and private keys, are used for encryption. In practice, end-to-end encryption is implemented via different technical standards depending on which form of communication – text message, audio/video exchange – and which messaging and video system is used. In addition, there are still **numerous technical limitations**, which would also stand in the way of possible interoperability. This firstly concerns the encryption of **text messages shared in groups (group chat)**, which becomes more and more complex as the size of the group increases. Solving this problem based on the new messaging layer security (MLS) standard is being tested in individual cases. Besides a new working group within IETF has been implemented. The* standard produced will allow for E2EE messaging services for

both - consumer and enterprise - to interoperate without undermining the security guarantees that they provided. Whether and to what extent and when the standard will be used by the whole industry may take some more time to turn out.

*End-to-end encryption is also subject to technical limitations with regard to **video conferences and webinars**. In general, end-to-end encryption requires participants to be technically able to provide and apply the necessary encryption functions. All participants have to be on the same security level. Conversely, end-to-end encryption is not possible if one participant fails to meet the necessary security level. This is the case, for example, if participants use a so-called **WebRTC client**. WebRTC is a protocol embedded directly in the browser, which can only end-to-end encrypt data between two end points. If there are more than two participants in a video conference, these end points are the user's end device and the service's server, which no longer meets the requirements of end-to-end encryption.*

*At present, end-to-end encryption cannot be technically linked to certain **functions** which users like to use in video conferences: These functions include, e.g., **joining a meeting via the public telephone network** or **recording meetings** using the hosting service. This is possible only if the service operator can access the data flow in order to include the audio caller or record the data. **Connecting certain external devices** (e.g. conference system devices based on the Session Initiation Protocol (SIP)) is not possible either using end-to-end encryption since various protocols would have to be synchronised for this purpose. Leading services expressly referred to these and other limitations, such as the **use of "assistants"**.*

*At present, it is not possible to ensure the technical security of large video conferences to host **webinars with several hundred participants** using end-to-end encryption. In this case, it is necessary to check whether the service provider operates a video service located in Germany and whether this service has been audited as to its technical security (for example by having been issued a BSI C5 certificate). Transport encryption and the secure operation of the video service in Germany should serve as a criterion in this context. It also has to be ensured that it is possible to establish the participants' identity with certainty ("authentication"). End-to-end encryption guarantees the integrity of the data transmitted. It makes sure that the data transmitted are protected but without prior unambiguous authentication, it is not possible to ensure who can receive the data.*

In the Bundeskartellamt's checklist, on which an assessment of the messenger and video services' quality of data protection could be based, **encryption is only one of several other criteria** of which consumers would have to gain an understanding. Against this backdrop, it seems neither reasonable nor expedient to put the responsibility for more data protection through competition on consumers alone, not even if the information were to be made available to consumers in an extremely condensed and simplified way. Measures to improve the quality of data protection must also include the services. In addition to effectively enforcing the applicable law, measures should thus be introduced which can strengthen data protection as a parameter of competition.

Assessment of the quality of data protection

In the Bundeskartellamt's current view, purely market-related measures may not be sufficient to help data protection gain some of the limelight among competition parameters and attract the

necessary attention. The state's involvement is likely to be necessary to bring data protection onto the big stage. For this purpose, the Bundeskartellamt proposes a **rating under state responsibility**. This rating is a transparent assessment of the quality of data protection provided by messenger and video services based on selected data protection and data security criteria, which is graded and published in a comparative ranking. The process is based on the credit rating of businesses, countries and institutions, which has been well established in the credit industry across the world for centuries. The rating could offer **motivation for both market sides**. It is first likely to trigger the greatest response by providers of messenger and video services. It can be assumed that many messenger and video services would like to avoid **publicly available negative reports or a lower ranking than the main competitor**. Data protection is not only "the law" – implemented in Germany and in Europe in the form of the GDPR – but it has meanwhile become a sensitive issue which is closely followed by the (professional) public and receives attention also in the political sphere. This situation has also been brought about by the ongoing debate on the conduct of some leading industry representatives and public reflections on state initiatives due to unwelcome practices and developments. However, it is also possible that users do not wish to be registered with a messenger and video service which **comes in last in the ranking**. Or perhaps one of their contacts would also prefer a messenger and video service involving a lower privacy risk than the service they have used so far. This also applies when action is taken on behalf of consumers: A rating published by a trustworthy body can serve as the **credible information professional "decision makers" or contacts** for the public at authorities or companies need to decide on a messenger and video service's compliance with the GDPR and thus its possibilities of use in their own institution.

Based on the present report, the Bundeskartellamt makes the following recommendations:

- The **enforcement of consumer rights should be strengthened**. Due to its technological basis in particular, the digital economy constantly poses new challenges for consumers, which are becoming increasingly difficult to capture despite the efforts made by all players. The Bundeskartellamt's competences and experiences in enforcing the law can provide a meaningful contribution in tackling the problems and creating solutions.
- Efforts to inform consumers, especially for the purpose of developing media skills, are to be intensified. All sections of the population should be a part of the **communication strategy relating to data protection**. A corresponding nationwide campaign should therefore use both internet-based digital media and traditional media, such as television.
- It would be a conceivable signal if the **public sector** were to increase the use of privacy-friendly messenger and video services. Contact persons and decision makers need reliable information on **messenger and video services' compliance with the GDPR** – especially with regard to those services which are not the focus of public interest. Institutions, organisations

and companies could therefore make such **written information, brochures and leaflets** available to their employees.

- **Interoperability** should not only be implemented in an **innovation-friendly** manner, but also in a **consumer-oriented** way. The already complex technical and legal context of data security and data protection is likely to become even more difficult to understand when interoperability is implemented. In all approaches and endeavours to create interoperability while also taking into account the technical challenges posed by this, the people responsible must, on behalf of the users, not lose sight of the **requirements for a secure consumer product**.