BoR PC03 (23) 09

DESIGNING INTEROPERABLE MESSENGER SERVICES

Response of the Federation of German Consumer Organisations (vzbv) to the public consultation on the “BEREC report on Interoperability of Number-Independent Interpersonal Communication Services”

3. February 2023

Impressum

Verbraucherzentrale
Bundesverband e.V.

Team
Digital and Media

Rudi-Dutschke-Straße 17
10969 Berlin

digitales@vzbv.de

INHALT

I. SUMMARY

With the entry into force of the Digital Markets Act (DMA) on 1 November 2022, an interoperability obligation for specific number-independent interpersonal communication services (NI-ICS), in particular messenger services, will be implemented within the European market for the first time.

The Body of European Regulators for Electronic Communications (BEREC) recently published the “Draft Report on Interoperability of Number-Independent Interpersonal Communication Services (NI-ICS)”, (BoR (22) 187) and opened the paper up for public consultation.

In its statement, the Federation of German Consumer Organisations (vzbv)[1] focuses on the aspects of the BEREC report concerning the DMA. This is because policy makers will implement and enforce the DMA obligations first. vzbv might comment on other topics at a later stage of their implementation process. As a representative of consumer interests vzbv thanks BEREC for the opportunity to contribute the consumer perspective on the report and has the following remarks:

- Before designating undertakings as gatekeepers, the European Commission should draft an implementing act with regards to the technical design of the interoperability obligation in Art. 7 DMA. The technical design should not solely be conceived by the gatekeepers themselves. Instead an independent body or the legislator itself should specify the technical design. The implementing act should at least specify some fundamental characteristics for the interoperability framework, e.g. whether an open protocol must be used.
- The interoperability obligation must ensure the highest level of data protection and data security. In particular, an interoperability obligation must not lead to a weakening of the level of data protection and data security for users who consciously choose a privacy-friendly service.
- Legislators must ensure that a standard uniform encryption protocol becomes mandatory in order to guarantee the confidentiality of the communication. This requires strong end-to-end encryption that preserves existing protection standards.
- User identification (user IDs) should not be based on telephone numbers or email addresses, but should be freely selectable by users within a defined scheme.
- vzbv welcomes the establishment of a High-Level Group whose task entails to regularly assess the implementation of the interoperability obligation under the DMA. The High-Level Group should therefore be endowed to enable it to identify upcoming needs to modify the interoperability obligation (IOO).

[1] vzbv published a discussion paper regarding the implantation of interoperability for messenger services in more detail in 2021: https://www.vzbv.de/sites/default/files/2021-05/21-05-18_vzbv_Diskussionspapier_Interoperabilit%C3%A4t_Messenger.pdf, 02.02.2023

II. INTRODUCTION

NI-ICS such as messenger services like WhatsApp, Signal or Threema have become an indispensable part of everyday consumer life. Consumers use them to quickly and cheaply send text and voice messages, photos, videos and other information over the Internet.

Consumers tend not to use a single messenger service but use, on average, three to four different services.[2]

WhatsApp, established in 2009 and taken over by Meta in 2014, had about two billion active users worldwide[3] – more than any other messenger service. As stated in the BEREC report, over three quarters of users within the European Union use WhatsApp and/or Facebook Messenger.[4]

Meta's dominant position may be detrimental to the market for messenger services as well as consumers. Although Meta, with its services WhatsApp, Facebook Messenger and Instagram, has repeatedly breached European data protection law[5] and designed terms and conditions that were not transparent[6], its services continue to attract the most users. That is the case even though the market offers numerous alternatives. Occasionally, there is a rapid jump in the numbers of users downloading alternative messenger services, mainly after scandals related to user information.[7]

A representative online survey from 2020 and 2021 by vzbv illustrates the pro-competitive effects of interoperability.[8] The survey shows that consumers would be willing to switch to another main messenger service if Messengers became interoperable: A third of all users (34 percent) could imagine switching to another main messenger service if they could reach all their contacts via that messenger. If users could reach all contacts via one messenger service, fewer respondents (68 percent) would opt for WhatsApp as their main service as compared to the current situation without this option (84 percent).

With the upcoming implementation of an interoperability obligation (IOO) triggered by the Digital Markets Act (DMA),[9] the European legislator has reacted to increasing market

---

[2] WIK: Oops, I texted again Kommunikationsverhalten in Deutschland (Oops, I texted again - communications behaviour in Germany), 2018, p.10.

[3] Statista: Statistiken zu WhatsApp, 2022, https://de.statista.com/themen/1995/whatsapp/#dossierContents__outerWrapper, 18.01.2023.

[4] BoR (22) 187: Draft BEREC Report on Interoperability of Number-Independent Interpersonal Communication (NI-ICS), 2022, p. 13.

[5] Federation of German Consumer Organisations: Mit dem Kartellrecht gegen die Datensammelwut von Facebook (Using cartel law to combat Facebook's data snooping), 2019, https://www.vzbv.de/pressemitteilung/mit-dem-kartellrecht-gegen-die-datensammelwut-von-facebook, 18.01.2023.

[6] Internet policy: The Federation of German Consumer Organisations wins in court: WhatsApp muss AGB auf Deutsch bereitstellen (WhatsApp must provide general business conditions in German), 2016, https://netzpolitik.org/2016/verbraucherzentrale-siegt-vor-gericht-whatsapp-muss-agb-auf-deutsch-bereitstellen/, 18.01.2023.

[7] Tremmel: Signal verfünffacht Nutzerzahl in kürzester Zeit (Numbers of Signal users quintuples in a short period), 2021, https://www.golem.de/news/weg-von-whatsapp-signal-verfuenfacht-nutzer-in-kuerzester-zeit-2101-153403.html, 18.01.2023.

[8] Verbraucherzentrale Bundesverband: Interoperabilität von Messenger-Diensten, Befragungen aus November/Dezember 2020 und April 2021, https://www.vzbv.de/sites/default/files/2021-05/2021-05-19%20Chartbericht%20Interoperabilit%C3%A4t%20von%20Messenger-Diensten_final.pdf, 02.02.2023.

[9] European Parliament and the Council: Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) 2022.

concentration, non-compliance with applicable data protection rules, and the regular occurrence of data scandals involving larger companies with regard to gatekeeping messenger services.

The implementation and enforcement of an interoperability obligation by the legislator should enable users of various messenger services to communicate with one another without having to switch or use multiple services (multi-homing). In theory, consumers could thus use a messenger service which offers a high level of privacy and security and still communicate with contacts who mainly use WhatsApp, for example. Hence, consumers could switch to more data protection friendly services more easily while competition on the messenger market would be strengthened.

From a consumer's point of view, three aspects regarding the design of an IOO are relevant: the identification and taking into account of users' interests as well as possible effects on competition and data protection. Ideally, the market for messenger services would be more consumer-friendly and feature an interoperable system that was legally and technically designed to promote sustainable and effective competition and market innovation. At the same time, it should guarantee a high level of data protection and data security.

III.INTEROPERABILITY UNDER THE DMA

For the implementation of the interoperability obligation, the DMA provides a time-bound procedure.

1. IMPLEMENTING ACTS AND TECHNICAL IMPLEMENTATION UNDER THE DMA

When the European Commission designates an NI-ICS providers as gatekeeper under Art. 3 of the DMA, the undertakings then have a specific timeframe to make their respective NI-ICS interoperable. Art. 7 of the DMA lays down that gatekeepers are required to publish a reference offer, in which they specify technical details and the terms and conditions of interoperability with its NI-ICS. Gatekeepers must publish the reference offer no more than six month after their designation as gatekeeper by the Commission.

Recital 64 of the DMA allows the European Commission to consult BEREC with regard to the gatekeepers' reference offers to ensure gatekeeper compliance with the IOO.

The DMA foresees various levers for the European Commission to influence (future) the design of the gatekeepers' reference offers and the technical implementation of the IOO:

Implementing Acts

Under Art. 46 of the DMA the European Commission has the possibility to adopt a variety of implementing acts. This includes implementing acts for determining the "form, content and other details of the technical measures" the gatekeeper shall implement to ensure compliance with the interoperability obligation in Art 7. Moreover, the European Commission is empowered to adopt implementing acts laying down the technical design i.e. the "operational and technical arrangements in view of implementing interoperability" for NI-ICS.

Delegated acts

To ensure the IOO is up-to date in the future Art. 12 (3) of the DMA empowers the European Commission to adopt delegated acts to amend the list of basic functionalities of NI-ICS for which gatekeepers shall enable interoperability under Art. 7. Art. 12 (4) allows the European Commission to adopt delegating acts to specify the manner in which those IOO are to be performed in order to ensure effective compliance with those obligations.

Technical standards

Art. 48 and Recital 96 of the DMA acknowledge that technical standards could be laid out for an interoperability obligation. They offer the European Commission the possibility to request European standardisation bodies to develop those technical standards.

From a user's point of view it is important that the technical design of an interoperability obligation is specified by an independent body or the legislator itself. This means for example, that an open protocol must be used or that end-to-end encryption must be implemented. It is important that a defined framework does not allow gatekeepers to tweak the technical design in their favour and thus allowing them to further expand their market and data power. The technical design of interoperable systems always has consequences for user interests, competition and data protection. It is not always possible

to tell a priori whether the advantages of the respective interoperability regime (or protocol) outweigh the disadvantages policy makers had to accept for going without interoperability.

Gatekeepers should not unilaterally decide over all aspects of the technical design. They have a strong incentive to design interoperability in their own favour to the detriment of consumers and competitors. Therefore implementing acts seem to be a reasonable tool to determine at least the fundamental principles and the broad framework of interoperability under the DMA.

Given the time frame that gatekeepers must publish their reference offer no more than six month after their designation as gatekeeper, in a best-case scenario the European Commission adopted an implementing act specifying the technical design before it designates the NI-ICS-gatekeepers. This would ensure that gatekeepers, from the start[10] on implement interoperability as intended by the legislator. As the designation of gatekeepers by the European Commission will likely happen in September 2023 this seems ambitious.

> Before designating undertakings as gatekeepers, the European Commission should draft an implementing act with regards to the technical design of the interoperability obligation in Art. 7 DMA. The technical design should not solely be conceived by the gatekeepers themselves. Instead an independent body or the legislator itself should specify the technical design. The implementing act should at least specify some fundamental characteristics for the interoperability framework, e.g. whether an open protocol must be used.

2. INTEROPERABILITY AND DATA PROTECTION

An interoperability obligation is intended to strengthen competition between messenger services by reducing network effects. On the one hand, this is associated with the hope of reducing market entry barriers for providers who place a higher value on data protection than it is the case with some of the established services. On the other hand, however, there is the fear that an interoperability obligation could have a negative impact on data protection. This would be the case if the existing level of protection of data protection-friendly services were lowered as a result of standardisation. Data protection levels could be undermined by the exchange of data that is necessary for communication between interoperating services. This applies in particular to the content of the messages, the user ID, any metadata and other data that are collected.

In principle, data protection can only be assessed in relation to the respective technical design of an actual interoperability obligation. However, various requirements can be defined in advance and the basic advantages and disadvantages of the various solutions can be presented.

For all design options a strong end-to-end encryption must be ensured, as a standard requirement for messenger services. This means that in the case of an interoperability obligation, regardless of its design, the standardisation of a uniform encryption protocol is necessary. Otherwise, it would be necessary for providers or a bridge to decrypt the message at one of the various transmission steps in order to forward it to the recipient

[10] The timeframe of the DMA requires that gatekeepers fully comply with the obligations in Art. 5, 6 and 7. by March 2024.

either in plain text or encrypted with another protocol. With such a decryption a provider could no longer guarantee the confidentiality of the transmitted content. Many messenger services already use the open "signal protocol" or implementations based on it, which is recognised as secure and state-of-the art by IT security experts.[11] However, it is crucial that interoperability does not lower existing protection standards, especially in end-to-end encryption, and that not only a procedure that represents the lowest common denominator becomes a standard.

The processing of user IDs, which cannot be avoided, is also relevant under data protection law. This is because the service via which a user sends a message always needs information about the recipient(s) in order to be able to deliver the message. If for example an interoperability obligation was to be implemented in the form of complete standardisation, this would also include user identifiers.

From a data protection point of view, user IDs should not be based on identifiers such as telephone numbers or email addresses, as these can easily be linked to further information. Instead, users should be able to freely choose their user IDs within a defined scheme and have different user IDs at their disposal if they wish - as is already common practice when using email services. One disadvantage would be that user IDs would have to be actively exchanged and contacts could not be easily found by uploading one's own address book - however, this practice is highly questionable from a data protection point of view anyway.

> The interoperability obligation must ensure the highest level of data protection and data security. In particular, an interoperability obligation must not lead to a weakening of the level of data protection and data security for users who consciously choose a privacy-friendly service.
>
> Legislators must ensure that a standard uniform encryption protocol becomes mandatory in order to guarantee the confidentiality of the communication. This requires strong end-to-end encryption that preserves existing protection standards.
>
> User IDs should not be based on telephone numbers or email addresses, but should be freely selectable by users within a defined scheme.

3. HIGH-LEVEL GROUP

In vzbv’s opinion the establishment of a High-Level Group is a good way to monitor the developments regarding the implementation of the interoperability obligation under the DMA. Markets and consumer needs can change fairly quickly for better or worse. Since there is a second regulatory framework with the “European Electronic Communications Code” (EECC) it is helpful to have an entity which regularly assesses the implementation and therefore can identify possible needs to modify the IOO in the future.

> vzbv welcomes the establishment of a High-Level Group whose task entails to regularly asses the implementation of the interoperability obligation under the DMA. The

[11] Kuketz, Mike: Messenger-Matrix (2021). URL: https://www.messenger-matrix.de, 18.01.2023.

> High-Level Group should therefore be endowed to enable it to identify upcoming needs to modify the IOO.