ADAPTING GDPR'S ARTICLE 25 TO MODERN COMMUNICATION: AN ANALYSIS OF WHATSAPP'S PRIVACY PRACTICES

Rainer Lukas
University of Library Studies and Information Technologies

Abstract: As digital communication becomes ubiquitous, the application of GDPR's principles of privacy-by-design and privacy-by-default has never been more critical. This study delves into the implementation of these principles by WhatsApp, a platform at the heart of global communication and scrutiny under the GDPR. By systematically analyzing GDPR legislation, WhatsApp's policy adjustments, and prevailing legal interpretations, this paper unravels the complexities and challenges of operationalizing privacy in a world where user data is a prized asset. Discover how WhatsApp's approach to privacy measures up to rigorous European standards, shedding light on broader implications for privacy in digital communication.

Keywords: GDPR, Privacy-by-Design, Privacy-by-Default, WhatsApp.

Introduction

The new European General Data Protection Regulation, known as the GDPR, came into force on 25 May 2018. Since then, the terms privacy-by-design and privacy-by-default should be familiar to interfaces between companies, which are obliged to comply with data protection requirements, and consumers. Article 25 of the GDPR refers to data protection by design and data protection by default: According to point 1, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons posed by the processing, the controller shall implement appropriate technical and organisational measures designed to implement the data protection principles effectively and to incorporate the necessary safeguards into the processing in order to meet the requirements of the Regulation and to protect the rights of data subjects. According to point 2, the measures must ensure that, by default, only personal data whose processing is necessary for the respective specific processing purpose is processed. The resulting basic principles of privacy by design and privacy by default will be considered and analysed below with regard to the WhatsApp messaging service. The aim is to analyse how the requirements for the principles of "privacy by design" and "privacy by default" can be interpreted more precisely with regard to Article 25 GDPR.

Technology design and default settings, data protection by design and by default, play a key role in data protection. The requirements under the GDPR must be updated on an ongoing basis.[1] With regard to implementation costs, the controller is not obliged to invest a disproportionate amount of resources if there are alternative and equally effective measures that bring the same benefits.

In the context of data protection regulations, the guiding principle is to protect personal information in social media from misuse. In this context, privacy means the right to allow people to decide for themselves when, how and for what purpose their information is made visible to others. Every user should be aware that by using these services, they consent to the right to the ideas and information they share online being passed on as soon as they are shared in the form of a message, a photo or a video. Ultimately, the user no longer has any control over these processes. With this in mind, the user's declaration of consent to the data protection provisions should be as simple as possible and still contain all the essential information so that the user can give their full consent on the basis of the information and in full knowledge of the consequences [1].

Research methodology

This study utilizes a qualitative research methodology, concentrating on document analysis to understand the application of GDPR's privacy-by-design and privacy-by-default principles within the operational framework of WhatsApp. This approach enables a detailed exploration of how theoretical legal requirements are translated into practical implementation in a widely-used digital platform.

WhatsApp serves as a case study due to its high profile and the significant legal and public scrutiny it has faced post-GDPR. The analysis focuses on changes in WhatsApp's privacy policy since GDPR's enactment and the examination of WhatsApp's use of end-to-end encryption as a privacy-enhancing technology to assess its effectiveness in securing user communications in line with GDPR standards.

Limitations

The study recognizes limitations such as the dynamic nature of legal interpretations and the inherent challenges in accessing comprehensive details on proprietary technologies and internal processing activities of private companies like WhatsApp. Moreover, the analysis is confined to publicly available documents and does not include proprietary or confidential corporate information.

Privacy-by-Design

The principle of privacy by design generally includes the requirement to involve data protection officers as early as the planning phase of an IT-based project [2].

Conceptualisation

Within the principle of privacy by design, a distinction must be made between two concepts: On the one hand, data protection by design and privacy by design. According to Article 25 of the GDPR, the controller is obliged to implement appropriate technical and organisational measures in order to comply with the data protection principles set out in Article 5 of the GDPR. Data protection by design specialises in this, while the term privacy by design is defined more broadly. This includes technological compliance with the Charter of Fundamental Rights of the European Union. At European level, the term is associated with the term "privacy-enhancing technologies", which covers the protection of data and privacy. This includes measures such as encryption, pseudonymisation, data minimisation and the elimination of any personal references [3].

The technical and organisational measures include all methods that a controller can use for processing.[1] The measures are suitable if the intended purpose can be achieved by applying the measure.

Definition

In view of the explanations on the content of the terminology presented above, it should be noted at this point that the term "privacy by design" can be used to define data protection through technology design. This includes the idea that the data protection requirements for processes within data processing can be complied with if the technical integration of data protection is already ensured when the corresponding system is created. A generally applicable definition does not yet exist, but rather the various implementations of the European member states. The absence of a national definition that can be subsumed leads to different interpretations and a lack of knowledge on the part of the implementing companies. Despite the increasing importance of the principle of conscious handling of personal data, there is a lack of precise specifications. However, it can be assumed that the core content will reach companies: all personal data must be protected preventively, not just after it has been collected and processed.[2]

Data protection requirements

It must be ensured, both technically and organisationally, that personal data is processed in accordance with the regulated requirements right from the planning stage. Article 25 of the GDPR requires that the data protection principles under Article 5 of the GDPR are taken into account, as well as the enforcement of data subjects' rights under Articles 12 – 22 of the GDPR. This must take into account the state of the art, the costs of implementation, the nature, scope, context and purposes, the likelihood and severity of the risks to the rights and freedoms of natural persons.[3]

The state of the art must be continuously measured against technical progress. If a responsible party does not adhere to the latest technological developments, this already constitutes non-compliance with Article 25.[1]

Practice-orientated case study

The current German Corona-Warn-App can be used as a practical case study. This app is a government-funded application in which the principles of privacy by design were already observed at the development and design stage. The personal data was transferred between the data subjects and the Robert Koch Institute using pseudonymisation mechanisms. In addition, the storage and processing systems are presented transparently. [4]

In order to implement privacy by design in a data protection-friendly manner, care should be taken to ensure that as little data as possible is collected, sorted and anonymised accordingly. These processes should be presented transparently in the information, monitored and continuously improved.[4]

Privacy-by-default

The privacy-by-default principle describes the data protection-friendly default setting that is intended to ensure the protection of the privacy of the respective user. In particular, users who are less likely to understand the technical requirements should be protected. This is generally regulated in Article 25 (2) GDPR. According to this, the controller shall implement appropriate technical and organisational measures to ensure that, by default, only personal data that is necessary for the specific purpose for which it is processed is processed.

This is also declared as the factory setting for some devices. The controller must configure these settings in such a way that initially only the processing that is necessary in the context of use is carried out automatically. The assessment of necessity is based on Article 6 (1), which generally means that no more data is collected than necessary and that it is not stored for longer than necessary.[1]

Conceptualisation

The term “privacy by default” can be understood to mean that no personal data may initially be processed in any system. If the user makes no other decision and declares this in the form of clicks and consents, they can assume that their privacy is guaranteed. [2]

Definition

Based on Article 25 GDPR and the explanations in the literature, it can be assumed that “privacy by default” is defined as the configuration of default settings for new technology with basic protection.

Data protection requirements

With regard to the principle of privacy by default, it must be ensured under data protection law that every action that processes personal data is technically and organisationally preset in such a way that only the data required for the specific processing purpose is processed. According to Article 25 (2) sentence 2 GDPR, this includes all actions relating to the processing of personal data, such as the amount, scope, duration of storage and its access.[5]

Practice-orientated case study

In each case, the principle of privacy by default is as follows: Users of social media platforms, for example, can decide for themselves whether they wish to consent to the unnecessary processing of data. The respective users have the option of agreeing to this processing or rejecting it individually. For example, after registering on a social media platform and confirming the data protection conditions, each user does not receive any further technical requests for consent to processing operations. One specific example is the default setting of not collecting location data when a smartphone is delivered. When using a technical function for the first time, a user can decide whether or not to consent to personal data such as location transmission when using the function.[6]

Results

At the beginning of January 2021, users of the messaging app WhatsApp received a pop-up notification informing them of an update to their “terms of use” that would share data with parent company Facebook. Users had to accept the new terms in order to continue using the app after 8 February. Privacy-enhancing technologies are used to cleanse or encrypt data from sensitive information in order to prevent conclusions from being drawn about individuals from the data in question. End-to-end encryption is applied when using

WhatsApp as soon as you talk to another person via the messenger. This is intended to ensure that only the person you are communicating with can read or see what has been sent and no one in between, not even WhatsApp itself. Technically, this works with a lock that is placed over the respective message and can only be viewed by a recipient with the generated key.[7]

Messages are stored in encrypted form on servers within the messenger for a maximum period of 30 days. WhatsApp cannot be used anonymously and therefore the messenger works with third-party providers and other Facebook companies, which means that personal data is passed on directly. With regard to this data protection issue, it is problematic that WhatsApp itself is divided into two companies. The first is WhatsApp Ireland Limited and WhatsApp LLC, the former of which is responsible for the European Economic Area and is therefore subject to the applicable data protection regulations, which are in line with applicable European law. The second company is located outside the European area of jurisdiction, which means that the provisions of European law do not apply directly. As a result, WhatsApp cannot be expected and required to meet the European standard with regard to the security of the use and processing of personal data.[8]

Currently, the privacy settings within WhatsApp are set in such a way that every user can see the exact time when a user was last online, whether they are currently online, the profile photo and information on read receipts without having to change them. The preset or changed status can also be viewed. It is also possible to be added to groups by other users. These preset settings can be customised by changing the conditions under the settings options of the respective device software. You can change who can see the profile photo, the time when you were last active, stored information or read confirmations. The option to be added to groups can also be customised. However, there is no indication that this can or must be set manually. It is only explicitly pointed out that you can deactivate read receipts in private chats, but not for group chats. Manual deactivation also applies to status messages. If you have switched off the read confirmation option, you will not be able to see who has viewed the status messages.

WhatsApp points out that there is no way to change whether other users can see whether you are currently online or writing something.[9]

The Hamburg Commissioner for Data Protection and Freedom of Information (HmbBfDI) objected to the handling of the data protection procedure for WhatsApp use. It issued an order with immediate enforcement due to urgency, according to which Facebook Ireland Ltd. is prohibited from processing personal data collected by WhatsApp if this is done for its own purposes. WhatsApp users were asked to agree to the new privacy policy, which gives Facebook more power over data sovereignty, by 15 May. After hearing

and analysing the facts, it was determined that the legal basis for this far-reaching data transfer was insufficient. There are both national and international versions that can hardly be distinguished from one another. There are contradictions in content that lead directly to misunderstandings. Even when categorising the content of the terms of use, it is not possible to fully understand what consequences agreeing to the terms of use actually entails for the user. Consent to these unclear and scattered declarations is not given voluntarily, but is virtually 'forced'. If consent is not given, use of the functions is not permitted without restriction. User consent is therefore obtained on the basis of a lack of clear, easily accessible, transparent information and a 'false' voluntariness. There is no basis under data protection law for the far-reaching amendment of the terms and conditions and no overriding interest in the processing of WhatsApp users' data due to conflicting interests in the rights and freedoms of individual users.

The new provisions serve to link the companies Facebook and WhatsApp even more closely together in order to improve the product and to be able to carry out advertising measures without restrictions. This constitutes use for its own purposes in accordance with the Data Protection Policy, which – despite requests – has not yet been reviewed by a supervisory authority. WhatsApp's behaviour therefore contradicts the conditions of the GDPR outlined above. The resulting problem of trust may have a lasting impact on the business model.[10]

According to statistics, the average social media user does not change their privacy settings. This directly demonstrates WhatsApp users' need for protection and the relevance of comprehensive default settings. In a study, problems with social network functions were analysed in terms of their data protection design. The results show that WhatsApp is not as secure as it seems for many users. Surveys show that many users are not aware of the security gaps and are also unaware of the options for comprehensively protecting their data, such as online visibility and accessibility of information. As a result, many users do not realise how openly they handle their data. Many do not realise that by changing the default settings, they could protect their data much more effectively from being disseminated, processed and passed on. Compared to other providers, WhatsApp may look less complex to use, but it only offers a few security precautions. Twitter and Snapchat allow users to better protect their information from the public. [1]

If users are continuously made aware of what it means to share their information in this way, they can better assess and regulate the extent of their data processing.

WhatsApp also has the problem that it is possible to receive messages from people you don't know. One possible solution to this would be a function that requires you to first send a message request to unknown contacts. Not only

can messages be sent from or to strangers, there is also a function that allows strangers to be added to WhatsApp groups. With regard to the granting of consent, there is a need for action at WhatsApp to optimise and guarantee data protection security for the reasons outlined above [5].

Conclusion

It should therefore be noted that the privacy-by-design principle enshrines principles that are intended to guarantee data protection as securely as possible. Privacy-by-default can be guaranteed by a functioning privacy-by-design by ensuring and taking into account data protection requirements at an early stage of development. This proactively prevents personal data collected at the beginning of a system's use from being stored or processed in such a way that it does not enjoy adequate protection. Such breaches are difficult to reverse, which is why a functioning system of data protection processes, data protection officers appointed as a precautionary measure, who immediately assume and thus supervise the processes in accordance with the standards within the Data Protection Regulation and regulated processes in the field of data storage and processing, is particularly important for companies. As already mentioned, this includes above all techniques for anonymisation and pseudonymisation, methods for encryption, limiting data processing to the necessary extent and the precise separation of required information with regard to the usability of a function. As described, the WhatsApp messenger service does not consistently fulfil these requirements.

With regard to the research question raised as to whether the WhatsApp messenger service complies with the aforementioned principles, it should be noted that, on the one hand, the European standardised data protection requirements cannot be demanded due to the different jurisdiction due to the local division of the company headquarters. Secondly, even before the introduction of the end-to-end encryption concept, the Messenger service forwarded the data collected from users directly to Facebook via the meta link and processed it in this way. In the context of the aforementioned aspects, the Messenger service was thus unable to guarantee a trustworthy basis for compliance with data protection principles. Companies should recognise data protection as a serious 'institution' as part of their business model and thus create trust by fully protecting all personal data of users and consumers. At the same time, users must be informed simply and transparently about what data is stored and processed, for what purpose and for how long. Users, on the other hand, should be aware of the consequences of privacy statements before giving consent and should act in the knowledge that the information shared after consent has been given will be processed and that the flow of information cannot be reversed regardless of consent.

The use of social media depends on the sharing and viewing of personal data. Under the GDPR, however, the purposes for which the data could be used (beyond the exchange of information via WhatsApp), how advertising processes run in the background or to what extent companies are associated with the exchange of information via WhatsApp should be regulated in a fully clear and transparent manner.

Notes

[1] **European Data Protection Board.** Guidelines 4/2019 on Article 25: Data protection by design and by default. 2020, // <https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_de.pdf> (5 May 2024)

[2] **Christian Thiel, Dominik Golle, Manfred Broy.** Privacy by Design as a win-win strategy for business and consumers, ZD.B Digital Dialogue, position paper, 2019, Bavarian State Ministry of the Environment and Consumer Protection.

[3] **Bundesverband Gesundheits-IT e.V., Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. & Gesellschaft für Datenschutz und Datensicherheit e. V. Arbeitskreis "Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen",** Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Article 25 DS-GVO), 2018, // <https://gesundheitsdatenschutz.org/download/privacy-design-default.pdf> (5 May 2024)

[4] **Jaap-Henk Hoepman.** Privacy Design Strategies (The Little Blue Book). 2022, Radboud University.

[5] **Thomas Hoeren, Ulrich Sieber, Bernd Holznagel.** Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschäftsverkehrs, 58th supplementary edition, 2022, C.H. Beck.

[6] **Peter Katko.** Checklists for the General Data Protection Regulation (GDPR) – Implementing, Mitigating, Auditing, 2020, C.H. Beck.

[7] **WhatsApp.** Information on end-to-end encryption, 2021, // <https://faq.whatsapp.com/791574747982248/?locale=de_DE> (5 May 2024)

[8] **David Oberbeck.** Is WhatsApp in companies compatible with the GDPR?, 2021, // <https://www.datenschutzkanzlei.de/ist-whatsapp-in-unternehmen-mit-der-dsgvo-vereinbar/> (5 May 2024)

[9] **WhatsApp.** Customise privacy settings, 2022, // <https://faq.whatsapp.com/1952310888335525/?locale=de_DE> (5 May 2024)

[10] **Martin Schemm.** Order of the HmbBfDI against Facebook, 2021, // <https://datenschutz-hamburg.de/pressemitteilungen/2021/05/2021-05-11-facebook-anordnung> (5 May 2024)

[11] **UC Berkeley.** School of Information. Privacy Policy Display, 2022, // <https://www.privacypatterns.org> (5 May 2024)

References

1. **Abdulmohsen S. Albesher, Thamer Alhussain.** Evaluating and Comparing the Usability of Privacy in WhatsApp, Twitter, and Snapchat, (IJACSA) International Journal of Advanced Computer Science and Applications, Volume 12, 2021, No. 8, Pages 251 – 259.
2. **Martin Rost, Kirsten Bock.** Privacy by design and the new protection goals, Datenschutz und Datensicherheit, Volume 35, 2011, Pages 30-35.
3. **Sheila Vasquez.** Privacy by Design and the Autonomous Vehicle, Privacy and Security, Volume 49, 2022, Pages 98 – 102.
4. **Alexander Dix.** The German corona warning app – a successful example of privacy by design, Datenschutz und Datensicherheit, Volume 44, 2020, Pages 779-785.
5. **Alisson Puska, Luiz Adolpho Baroni, Maíra Codo Canal, Lara S. G. Piccolo, Roberto Pereira.** WhatsApp and false information: a value-oriented evaluation, 2020, IHC '20.

About the Author

Rainer Lukas holds a Master's degree in Law from the University of Central Lancashire, an MBA from Anglia Ruskin University in Cambridge, the Intermediary Exam in Law from University of Münster and numerous certificates in the area of Informatics, Data protection and Cyber security where he is currently involved in various research activities and projects. He was a visiting scholar at the China Academy of Social Sciences and he is a lecturer at the International University (IU) and FOM University of Applied Sciences for Economics and Management. Additionally, he is a PhD student in the University of Library Studies and Information Technologies in Sofia.

To contact the Author: rainer.lukas@gmail.com