Position Paper

Bitkom views on EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects

24/05/2019

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

Introduction and Overview

Bitkom welcomes the opportunity to comment on the European Data Protection Board's (EDPB) draft Guidelines on the processing of personal data under Article 6(1)(b) of the GDPR in the context of online services. 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.

We therefore appreciate that the EDPB published the draft Guidelines on the use of the legal basis of Article 6(1)(b) GDPR.

Overview:

1. Summary

We suggest broadening the scope of the Guidelines to include the processing of personal data under Article 6(1)(b) in the context of offline services as well.

We would like to highlight the following aspects:

- In our view, it is necessary to clarify that multiple legal bases can apply at the same time.
- The interpretation of "necessity" need to be amended and made more flexible.
- The Guidelines should include Guidance on the relationship between Article 6(1)(b) and Article 6(1)(f) as well as the legal bases for processing under the upcoming ePrivacy Regulation.

2. Scope of Article 6(1)(b) GDPR

2.1 "Necessity"

Article 6(1)(b) GDPR provides a lawful basis for the processing of personal data to the extent that "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract". As the draft Guidelines rightly state, this supports the freedom to conduct a business, which is guaranteed by Article 16 of the Charter. The scope of this legal bases should, however, not be understood too narrow. The wording of the GDPR in comparison to Article 6 of the draft ePrivacy Regulation and Recital 13 of the Digital Content Directive shows the GDPR´s intention of including more business models into Article 6(1)(b) GDPR. "Necessary" for performing a contract has to be understood which a view on the whole contractual concept. If part of the contract is the supply of a service free of charge (monetising it via advertising f.i.) the provision of such a free service leads to the data processing being necessary for performing such a contract.[1] The freedom to conduct a business includes the guarantee for contractual freedom and the freedom to define and build a business as long as it operates within the law. Such freedoms are essential for our economy and driving innovation. It is therefore imperative that companies are free to define how

[1] See: https://www.lda.bayern.de/media/baylda_ds-gvo_12_advertising.pdf.

they want to offer their services – including the way to monetise their business model. The GDPR itself provides the safeguards necessary to balance the interests of business and users: the risk-based approach, compliance with transparency obligations and user rights – to name but a few.

In our view, there is no need for the draft Guidelines to restrict Article 6(1)(b) GDPR to situations where it would be altogether impossible to deliver or supply a service without the processing of the specific personal data in question. In recital 44, the GDPR explicitly states that processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract. This suggest a broader scope and is also supported by general contract law where the contracting parties can shape their contractual relationship as well and are not limited to purposes and measures that are strictly necessary without looking at the context of the contract. In should also be noted that if the narrow interpretation suggested in the draft Guidelines persists, the contracting parties may end up with contracts that cannot fully be performed since the aim of the contract would require more data processing than what would fall under the definition of the Guidelines.

2.2 Distinction between Articles 5 and 6

The draft Guidelines also draw a connection between Article 5 and Article 6 that is not supported by neither the intention nor the wording of the GDPR. In para 1, the draft Guidelines state that Controllers must take into account the impact on data subjects' rights when identifying the appropriate lawful basis so as to fully respect the principle of fairness. However, the principles laid down in Art. 5(1)(a) GDPR are connected to the data processing and not the selection of the appropriate legal bases. These two separate steps should not be merged which is why the draft Guidelines should reflect this distinction and should therefore be amended.

2.3 Purposes of contractual performance

In para 16 the draft Guidelines state certain purposes stated in contract terms, f.i. 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will as a rule not be considered to be specific enough to describe the purpose of a contract. In our view, such purposes do not constitute unclear terms.

With regard to ÍT-security purposes Art. 32 GDPR has to be taken into account as well. The companies are obliged to guarantee the security of the processing. The company is obliged to

establish a procedure for regular review assessment and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing. A detailed description of the chosen measures is not sensible, since by the naming of detailed measures, the security measures would be made vulnerable again. This would also endanger achieving what the provision aims to: the security of the data. From this point of view, naming ´IT Security purposes´ in the description of purposes to the must be sufficient.

Furthermore, we think that the EDPB's view on "service improvement" (Part 3.1, numbers 45 seq.) is too narrow. User's expect the improvement of an existing service, e.g. in terms of a better connectivity or a higher level of security. To include improvements in contractual terms can be objectively necessary, e.g. if beta version or MVPs are offered. Here a differentiated view - at least for service improvements, but in some cases also for the development of new functions.

Additionally, we suggest providing clarification regarding finance and resource planning, which are necessary on the one hand to ensure service to the customer in the online environment and thus necessary for the provision of contractual services to the customer (e.g. purchase of servers, purchase of licenses). Such a planning presupposes the analysis of the actual state and should therefore not be confused as "service improvement". A too narrow interpretation of "service improvement" therefore has a negative effect on competitiveness. It is not helpful to refer to other legal bases such as "legitimate interest" or "consent", as this can be accompanied by the right of objection/revocation with regard to data processing. However, planning is necessary for the entire customer base in order to be valid. Furthermore, the legal basis "legitimate interest" cannot be chosen for data processing operations subject to the restrictions of Art. 9 DSGVO and this could lead to additional damage to the competitiveness of the companies concerned. Recital 4 should be taken into account in this regard: The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This includes the freedom to conduct a business.

Describing each purpose in too much detail would rather overburden the user with even more information and extend every data protection notice. Furthermore, data protection notices need to be kept future proof and practicable for the businesses that are using them. We would therefore suggest including the possibility of using abstract terms to describe the purposes and include examples to achieve transparency for the user.

2.4 Application of several legal bases

We disagree with the draft Guidelines assessment in para 39 that it is generally ´unfair´ to swap legal bases if one ceases to exist. This statement is not supported by the GDPR as Article 6(1) provides that processing shall be lawful only if and to the extent that at least one of the following applies(...). Article 17 I b GDPR furthermore explicitly includes the scenario where the data subjects withdraws consent and there is no other legal ground in place: *the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing.* To reflect the GDPRs provisions and intention the Guidelines should be amended in this regard.

As the same data processing can serve multiple purposes it can be based on several legal bases (which is explicitly supported by Article 6(1)). For example, an controller logging users' IP addresses may rely on Article 6(1)(b) GDPR insofar as the logs serve to protect the users' own user accounts (i.e., fulfilling the provider's duty of care towards the personal data stored in registered user accounts), and Article 6(1)(f) GDPR insofar as the logs serve to protect the website offering (i.e., only in the provider's own interest). In this example, the controller can rely on Article 6(1)(b) and (f) GDPR as compatible legal bases for the same processing. The same is true for pre-contractual provision of test-versions as many providers offer not only paid or free services on the Internet on the basis of permanent contarcts. They also usually offer time-limited test or demo versions for contract initiation. Here, too, personal data must be processed, because during this phase the enterprise has a legitimate interest to provide the user with the best services possible to conclude the contract at the end of the test-phase. The prospective customer also expects to be supported during the pre-contractual phase in order to evaluate whether the product and the provider fits his needs. In addition to the legitimate interest of the provider consent by the user is likely to provide grounds for processing.

In conclusion, we think the Guidelines should be amended, because as long as the controller provides for information regarding the legal bases and fulfils his transparency obligations we do not see reason for the restrictions the draft Guidelines propose.

3. Scope of the Guidelines

In our view, it is necessary to broaden the scope of the draft Guidelines as well. The Guidelines should include the processing of personal data under Article 6(1)(b) in the context of offline services as well.

The Guidelines should also include Guidance on the relationship between Article 6(1)(b) and Article 6(1)(f), include an assessment of Article 6(4) as well as the legal bases for processing under the upcoming ePrivacy Regulation. This is of particular importance, because the draft ePrivacy Regulation does not permit the controller to rely on "legitimate interests" for processing and it is therefore important to interpret Article 6(1)(b) GDPR in a way that will harmonize with the alternative legal bases under the upcoming ePrivacy Regulation. The Guideline refers to legitimate interest as an alternative legal ground but the proposed ePrivacy Regulation does not include the possibility of processing personal data for the performance of contract, for the legitimate interests of the controller or process them for compatible purposes. The e-communication service providers will therefore not be able to process personal data for service improvement or network optimization. The narrow interpretation of the legal ground ´performance of a contract´ in combination with the insufficient draft of the ePrivacy Regulation is not feasible for e-communications service providers and puts them into a situation where they cannot provide best-in-class service to their customers.

With its interpretation, the Guideline is limiting the offering of services, such as those related to AI and Machine Learning, whose value proposition implies to constantly process data in order to anticipate the needs of customers and constantly develop the service according to those needs.

We therefore recommend amending the Guidelines in this regard and include a note to the effect that the Guidance will be revised, once a final draft of the ePrivacy Regulation has been agreed.

We also suggest including guidance on the application of privacy by design and privacy by default as defined by Art. 25 of the GDPR, in particular with regards to the topic of data processing on the basis of an agreement to general terms and conditions or the signature of a contract, rather than through the data subject's consent. The Guidelines should provide for more clarity with regard to open questions on how to apply the data minimisation requirement which is only briefly mentioned in point 16 of the guideline but has led to many questions since the one years the GDPR has been in place.

In para 8 the draft Guidelines note that Data protection rules govern important aspects of how online services interact with their users and that other rules apply as well. Regulation of online services involves cross-functional responsibilities in the fields of, inter alia, consumer protection law, and competition law. The EDPB concludes that considerations regarding these fields of law are beyond the scope of these guidelines. We think it would improve the Guidelines and their feasibility if there would be more exchange between data protection, contract law and competition law experts due to the overlaps between the regulatory frameworks. Looking at the new Directive for Digital Content and its provisions on contracts that are provided without monetary compensation but with data as a counter performance this overlap now found its way into another EU Regulation. New and interdisciplinary considerations have to play a bigger rule when applying and interpreting all these rule sets.