Bundesverband E-Commerce und
Versandhandel Deutschland e.V.
www.bevh.org

- Bundesverband E-Commerce und Versandhandel Deutschland e.V. (bevh) -

Position Paper on the EDPB's Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR

Berlin, 20th November 2024

Contact: Alien Mulyk, Manager Public Affairs EU & International, alien.mulyk@bevh.org

Bundesverband E-Commerce und Versandhandel Deutschland e.V. (bevh) represents the interests of online and mail order retailers active in Germany of all sizes and trade channels (online, multichannel, catalogue, TV shopping, platform dealers and operators). The members of bevh represent more than 75% of the entire industry turnover. In addition, more than 130 service providers from the e-commerce sector are affiliated with our association.

I. General remarks

In practice, in Germany, it is already difficult for companies to invoke a legitimate interest as there are overlaps, particularly with the UWG (German law against unfair competition). Relying on a legitimate interest is therefore subject to very narrow limits. In practice, the consumer's interest is de facto always rated higher by the authorities, so that it is not possible for companies to invoke a legitimate interest with regard to advertising measures. Without explicit consent, it is therefore very difficult to implement advertising measures at all. Therefore, we welcome, that according to the EDPB's guidelines there is no hierarchy between the different legal bases in Article 6(1) GDPR. We also welcome that generally a wide range of interests is considered legitimate. However, we are still afraid that the guidelines will make it more complicated to use legitimate interest as a legal basis not only for advertisement purposes but also for security measures.

II. Balancing Exercise & Methodology

The GDPR assumes that assessments are usually made on a broader basis as it allows in Art. 21 that individuals can object in case their situation differs from what can be normally expected. This is particularly true, as the assessment needs to happen prior to the data processing. At this moment, the company has no information on the individual data subjects and their particularities. Thus, the guidelines contradict the provisions of the GDPR by requiring that a balancing exercise

must be done for each processing before it is carried out (para. 7). In addition, there is no legal basis in the GDPR that justifies that the DPO must be involved in the assessment (para 12).

Moreover, the EDPB should not generally prejudge as in para. 30 if a controller might be able to demonstrate the necessity of the processing when it relies on third party interests. This is, as constantly held by the CJEU, subject to a cases-by-case assessment.

In its guidelines, the EDPB doesn't seem to recognize that companies can have other than financial interests such as improving their services or to benefit the environment. However, there are various different purposes for which companies rightfully invoke legitimate interest e.g. fraud detection, reducing returns by e.g. improving size recommendations and fit predictors or improving the customer care service. Accordingly, the EDPB should not only give examples of negative effects on customers, but also of positive ones that justify invoking legitimate interest. In this context, it is also important to point out that there are differences between the types of data within data categories. Location data for example should not in general be excluded from the types of data that can be processed when invoking a legitimate interest (para 40) - it depends on the specific data used: static location data for example is less intrusive than the collection of GPS data collected over a long period of time by mobile phones and has no significant negative impact on the data subject's rights, freedoms and interests. This is also the case for financial data, when it comes to data like the bank identification number for example.

Moreover, many obligations in the GDPR already reduce the impact of the processing such as the right to object and delete data, transparency, implementation of strong security measures, minimization of data and retention periods. This should also be considered in a balancing test. However, the principle of data minimization should not be used to undermine the possibility of invoking a legitimate interest. But there should be a positive assessment if data controllers limit their processing to less data than would be justified.

There is also no definition of "going beyond" in the GDPR. Retaining this wording in para. 34 of the guidelines makes matters thus even more complicated. Broader emotional impacts are also not covered by the GDPR and seem to be more part of the discussion on the Digital Fairness Act (par. 46). It is also unclear how the data controller should estimate this impact. Finally, there is no legal basis in the GDPR for the data subject to obtain information on the balancing test upon request (paragraph 68) also not in Art. 13.1d. This also holds true for para. 71 that requires the data controller to ask for further specification of the request in case the data subject didn't elaborate much on its particular situation that led to the objection of the processing of its data based on legitimate interest.

III. Contextual elements & Reasonable Expectations

If the user is offered coherent services with different features in the responsibility of a single company group, the data subject can expect the processing of data. If the same service is accessed from different devices or different services that have a recognizable connection, the processing of data will not be a surprise for the consumer either. The customer even expects a unified personal experience across these services and devices. It is important to consider the individual case, for which para. 120 of the guidelines leaves however no room. Advertising similar products of those that the customer has already bought as suggested in the guidelines (para. 120) is very old-fashioned and is also not in the interest of the consumer. Thus, instead of recommending this outdated and inefficient marketing technique, the guidelines should rather focus on more relevant and realistic examples that take into account up-to-date customer-centric marketing approaches. As add analytics and measuring engagement such as counting ad-attributed purchases and providing aggregated counts to advertisers to demonstrate effectiveness are not intrusive, they should be added to the list of practices with little impact on data subjects. As "tracking" is not defined in the GDPR in contrast to profiling, the EDPB should not refer to it in the guidelines.

It can be expected that people know that their data is being processed in some parts as common practices shape their expectations. It is thus not understandable why the EDPB in para. 53 considers that the presence of information on the processing is not relevant for the expectations of the data subject. It should also be possible for the data controller to demonstrate the data subject's understanding by studies etc. Also here, rather than just providing information on what would be not compliant, positive examples of what companies could do to ensure that users are sufficiently informed would be useful.

IV. Fraud prevention & Security Measures

Fraud prevention constitutes a legitimate interest according to recital 47 GDPR. Thus, the "may" needs to be deleted in para. 100 of the EDPB's guidelines and it should be recognized that **any** type of fraud can be a basis for legitimate interest. It is positive that para. 103 rightly recognizes that fraud prevention can also serve the partners of the data controller. It is however, not clear which data processing operations are necessary to effectively combat crime as the activities of criminals are continually evolving. Therefore, future interests should also be qualified as legitimate interest.

As it is not possible to predict what information will be necessary for the effective protection of the business, their business partners and customers, para. 127 of the guidelines is potentially in contradiction with the obligations in Articles 25 to 32 of the GDPR. Moreover, data processors still have to be able to fulfil their obligations also under other legislation such as the Cloud Act. In addition, it is not understandable why, when a company is victim of a cyber-attack the EDPB

applies a very strict approach to sharing the perpetrator's online identifiers with the authorities (para. 132). At least, the EDPB should recognize that misuse and criminal behavior by a data subject can be considered in the balancing exercise.