Ecommerce Europe feedback on Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR

Preliminary comments

Ecommerce Europe is the united voice of the European Digital Commerce sector, representing the interests of companies selling goods and services online to consumers in Europe. Ecommerce Europe welcome the drafting of these Guidelines as they aim to clarify and assist data controllers in implementing a general and complex standard. They set out three cumulative conditions for a controller to be able to base its processing on legitimate interest, while recognising that assessing these conditions is not an easy exercise, particularly when it comes to balancing the interests of the controller against the rights of the data subject. The European Data Protection Board (EDPB) therefore provides guidance on how to assess these criteria, including in specific contexts such as fraud prevention, direct marketing and so on. We welcome the non-exhaustive criteria and examples provided for these strategic and central processing operations.

While we believe that the Guidelines provide a valuable contribution to the interpretation of the GDPR, we generally find that the extensive nature of these Guidelines, particularly given the relatively brief treatment of the concept in the GDPR's articles, may be disproportionate. In general, the Guidelines should focus on the importance of Article 6(1)(f) GDPR for businesses, as well as the necessity to apply the **principle of proportionality** to ensure that a balance with all fundamental rights, freedoms and principles can be achieved. However, the wording of the Guidelines may narrow the scope of Article 6(1)(f) GDPR more than necessary, while it should focus on the potential of Article 6(1)(f) as a valuable legal basis that can serve as a central standard for data processing operations. Furthermore, the Guidelines should also aim to strike a balance between providing clear guidance and avoiding excessive bureaucracy with new extra requirements different from the ones covered in the applicable law. It is crucial that data controllers are able to implement the Guidelines in a **practical manner**. However, we fear that the Guidelines will make it more complicated to use legitimate interest as a legal basis.

I. Introduction

We welcome the emphasis on the fact that there is **no hierarchy between the different legal basis** in Article 6(1) GDPR, underlining that Article 6(1)(f) is neither a less valid nor less important legal basis in comparison to other legal bases like consent.

The Guidelines state that the balancing exercise must be carried out "*for each processing before it is carried out*" (para. 7), and that "*when personal data are processed for different purposes the processing for each of those purposes must fall within one of the cases provided for in Article (6)(1) GDPR*" (para. 10). These requirements make it particularly complicated, and not a scalable process, to rely on Article 6(1)(f) GDPR. The requirements defined here are very granular, and a differentiation and subdivision has to be considered for so many cases, that a meaningful assessment to enable a number of use cases is no longer possible. In Article 21 GDPR, individuals can object if their situation differs from what can normally be expected. Therefore, the GDPR assumes that assessments are usually made on a broader basis. This is particularly

true as the assessment must take place prior to the data processing at a moment where there is no information on the individual data subjects and their specificities.

II. Elements to be taken into account when assessing the applicability of Article 6(1)(f) GDPR as a legal basis

As a preliminary remark, we would like to stress that there is no legal basis in the GDPR that justifies that the DPO must be involved in the assessment of Article 6(1)(f) applicability, as stated in paragraph 12.

- **1st step: pursuit of a legitimate interest by the controller or by a third party**

Ecommerce Europe welcome that in general, a wide range of interests can be considered legitimate (para. 16). However, we would appreciate the Guidelines to provide positive examples, in which legitimate interest can be used in the context of Recital 47, i.e. when the data subject is a customer or provides services to the controller. It is unfortunate that the Guidelines only exemplify this scenario with three cases in which legitimate interest cannot be used (para. 18).

- **2nd step: analysis of the necessity of the processing to pursue the legitimate interests**

Regarding the assessment of what is "*necessary*" (para.29), the guidelines should specify, with practical examples, cases in which it is understood that there is an objective need, and cases in which it is not a need, but a "useful" processing activity for the controller. Moreover, the Guidelines state that the condition relating to the need for processing must be examined "*in conjunction with the 'data minimisation' principle*" (para. 29). We believe that the data minimisation should not be seen as an end in itself or in isolation from the assessment context, but meaningfully integrated into the legitimate interests assessment in such a way that the pursuit of an interest initially recognised as legitimate is not undermined by the imposition of excessive restrictions. Lastly, it must be underlined that the necessity assessment must be done on a case-by-case basis especially if the data processor relies on third party interests, and that this should not be prejudged by the EDPB (para. 30).

- **3rd step: Methodology for the balancing exercise**

Ecommerce Europe welcome the clarification that "*the purpose of the balancing exercise is not to avoid any impact on the interests and rights of the data subjects altogether*" (para. 33). We believe that this useful clarification should be carefully considered when introducing further restrictions on data controllers.

In paragraph 38, the EDPB does not seem to recognise that companies may have interests other than financial, such as improving their services or benefiting the environment. It focuses only on obvious interests described in general terms. In fact, there are many questions connected with other "interests", such as user convenience (e.g. design of the interface), security of service (e.g. login options, KYC options), user experience (e.g. satisfaction with presented offer, easy access to service or information). These actions are taken not only in the interest of controllers but also in the interest of users.

Accordingly, the EDPB should not limit itself to providing examples of negative effects on customers when assessing the impact on the data subject (para 39). We would welcome for the Guidelines to elaborate on positive effects which can for instance be: detecting and closing security gaps at an early stage, detecting fraud attempts, making a service more inclusive, reducing the environmental impact of the business model, improving order management and transaction convenience, improving size recommendations and fit predictors, improving the customer care service or customer journeys, etc.

Regarding paragraph 39, we would welcome the EDPB to mention that the assessment should focus on various **but not purely theoretical** ways in which individual may be affected. The difference between "*potentially"* and "*theoretically*" has a big impact on practical assessment, because there is often some anxiety, whether the "potential" scenario means only typical scenarios connected with given context or it means everything which might occur (e.g. so called corner cases). Direct exclusion of purely theoretical scenarios will put some more visible and reasonable limits on this assessment.

Regarding the balancing test, it is important to recall that many obligations in the GDPR already reduce the impact of the processing like for instance the right to object and delete data, transparency, implementation of strong security measures, minimisation of data and retention periods.

We would recommend paragraph 44 to differentiate between "*child at a young age or with a certain level of cognitive ability"*. Indeed, the reference to children without distinguishing age category is problematic as it forces controllers to treat 10,13 or 16 year olds in the same way and with similar caution, while the differences in knowledge and ability are obviously different. A direct recommendation that controllers shall pay special attention to the youngest users while also considering the average cognitive differences associated with a child's age would be very helpful.

Furthermore, since the GDPR does not define *"going beyond"*, keeping this wording in paragraph 34 adds an additional layer of complexity. Similarly, the notion of "*broader emotional impacts from a data subject losing control over personal information"* (para. 46) is not covered by the GDPR. We believe, it should be linked to a specific right or interest to avoid misuse and misunderstandings. It is also unclear how the controller should estimate this impact, which seems to be more part of the Digital Fairness discussion. We also find the wording in the last example (para. 46) overly broad, as it covers both ordinary situations inherent to the modern functioning of the internet, and activities where advertising or profiling is very intrusive. Using the wording "*reasonable sense of feeling*" would exclude purely theoretical situations.

- **Reasonable expectations of the data subject**

The Guidelines state that "*the fact that certain types of personal data are commonly processed in a given sector does not necessarily mean that the data subject can reasonably expect such processing"* (para. 52). However, it is generally understood that common practices in a particular sector naturally shape customer expectations. Additionally, it is important to consider that this is an evolving process as data processing operations that may have been less familiar or anticipated by customers a few years ago might now be widely recognised and expected as part of certain services.

We also have concerns regarding the Guidelines' selective approach in paragraph 53, which treats the presence of information as irrelevant to a data subject's expectations while viewing the absence of information as relevant. It can be expected that individuals know that their data is being processed as common practices shape their expectations. It is therefore difficult to understand why the EDPB considers that the existence of information about the processing is not relevant to the expectations of the data subject. We would also welcome positive examples of what would be compliant.

The Guidelines state that "*contractual provisions regarding personal data may have a bearing on the reasonable expectations of data subjects*" (footnote 61). However, the impact of contractual provisions on a data subject's reasonable expectations can only play a role when data processing is at the core of the contract fulfilment, in which case the data controller will rely on Article 6(1)(b). For cases relying on Article 6(1)(f), data processing provisions should be laid down in a privacy notice rather than in the contract itself. Granting higher importance to information in a contract within an Article 6(1)(f) GDPR context is misleading.

Regarding the "*proximity of the relationship*" as a contextual element to be considered in the assessment (para. 54), it is understandable that completely different services offered by the same controller or under its

responsibility should be taken into account with regard to the expectations of the data subject. However, this strict distinction is not appropriate where the data subject is clearly offered coherent services with different features that are the responsibility of a single company group.

Lastly, regarding the characteristics of the "*average*" data subject (para. 54), it follows from Article 21 GDPR that the general considerations of the balancing of interests must be based on generalised considerations. It is also understood that individual deviations from them are not to be taken into account by the data controller from the outset, but can be asserted individually by the data subject by way of an objection. In addition, the data controller often does not have such detailed information regarding individual data subjects at the stage of weighing up interests, which has to take place before the data processing is carried out. Lastly, the "*average*" will vary depending on the environment in which the data users operates. E.g. a registered user with a history of online shopping is likely to have greater familiarity with e-commerce and the platform they use compared to someone new to the internet.

- **Finalising the balancing test**

Compliance with generally applicable obligations to fulfil information obligations or to implement and maintain security controls cannot be considered an additional protective measure. Nevertheless, we do not consider it out of the question that this also applies to efforts in terms of data minimisation. Of course, this principle applies in any case of data processing, regardless of the legal basis. Nevertheless, this data processing principle is one that is particularly difficult to grasp and requires interpretation. There is no black or white here. Accordingly, there should be a positive assessment if data controllers limit their processing to less data than would be justified.

III. Relationship between Article 6(1)(f) GDPR and data subject rights

- **Transparency and information to be provided to data subjects**

The Guidelines' primary purpose is to assist controllers in assessing whether legitimate interest can be invoked as a valid legal basis for their processing of personal data (para. 3). Furthermore, the GDPR and subsequent CJUE rulings have enhanced the significance of the legitimate interest lawful basis (para. 5). However, paragraph 68 introduces a set of obligation not explicitly stated in the GDPR or CJUE rulings:

- *Pre-collection balancing-test transparency*: providing data subjects with information from the balancing test before collecting their personal data.
- *Post-collection balancing-test information*: offering data subjects the opportunity to obtain information on the balancing test upon request.

While it is acknowledged that legitimate interest may necessitate additional safeguards beyond the GDPR's strict requirements, the above obligations, inferred by the EDPB from GDPR principles like fairness, transparency, and accountability, are presented as "essential" for compliance. We respectfully request that the EDPB reconsider these obligations as **additional safeguards** that data controllers may consider in the balancing test, rather than mandatory requirements for GDPR compliance.

Furthermore, while it is suggested that "*information to the data subjects should make it clear that they can obtain information on the balancing test upon request*" (para. 68), it is worth noting that there is no legal basis for this within GDPR.

- **Right of access**

As part of exercising the right of access, paragraph 70 recommends that data controllers provide information on the legal basis for the processing, even though the GDPR does not require this. We welcome the desire to ensure that data subjects are fully informed about the personal data that a company holds about them and the processing carried out on it. However, these information requirements relating to the

legal basis may be complex to understand for consumers, who are already confronted with a very large amount of information and who do not necessarily have the expertise to assess the legality of a processing operation. We fear that this will generate a number of questions, sometimes taking the form of debates between data subjects and controllers on the legality of the processing. There is a risk that data controllers will then have to devote significant internal resources, particularly human resources, to this.

- **Right to object**

Paragraph 71 suggests that if a data subject objects under Article 21 GDPR without providing much detail, the request should not be dismissed, but the controller may ask for clarification. However, we do not find the legal basis for this requirement in the GDPR. Furthermore, we welcome the initiative to clarify and define the concept of "*compelling legitimate interest*" (para. 73), as it has been considered a vague legal concept. However, we would welcome for the EDPB to also provide the elements to be taken into account when analysing whether a legitimate interest can become compelling. It would also be welcome if a list of compelling legitimate interest scenarios were included, as well as the essential elements to be gathered in each of them, in order to check the validity of such compelling legitimate interests. While the conditions we request to be included may not be determinative of whether a legitimate interest is compelling, they will undoubtedly help data controllers to clarify which elements should be considered.

- **Automated individual decision-making, including profiling**

There are already interpretations suggesting that the last sentence of paragraph 81 entirely rules out the possibility of automated decision-making to be based on legal provisions. A clarification that this applies specifically to the direct reference to Article 6 of the GDPR, without excluding other provisions, would cast this doubt.

- **Right to rectification**

We would welcome the EDPB to explore in more details the implications when it is said that "*the data subject may have a legitimate interest in having their data rectified*" (para. 86). The legitimate interest indeed plays an essential part in the erasure right, but we are not entirely sure what are the implications when it is about legitimate interest, aside from the examples provided at the end of the paragraph 86 in which it is clear that the interest is not legitimate. Another form of interplay between the rectification right and the legitimate interest could be those scenarios in which the data controller is keeping stored information for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the European Union or of a Member State. For instance, a data subject may want to rectify information stored based on legitimate interest for those purposes described, and such situation could jeopardise the interest of the data controller in case using such information afterwards for those purposes become necessary.

IV. Contextual application of Article 6(1)(f) GDPR

1. Processing for the purpose of preventing fraud

Fraud prevention constitutes a legitimate interest according to recital 47 GDPR. Therefore, the "*may*" in paragraph 100 should be deleted. It should also be recognised that **any type of fraud** can be a basis for legitimate interest. It is positive that paragraph 103 rightly recognises that fraud prevention can also serve the partners of the data controller. However, it is not clear which data processing operations are necessary to effectively combat crime, as the activities of criminals are constantly evolving. Therefore, **future interest** should also be qualified as legitimate interest. We would also welcome more guidance on how the reference to legitimate interest in combating fraud should be included in the privacy policy, e.g. whether or not the type of fraud should be specified.

2. Processing for direct marketing purposes

Compliance with specific legal requirements that preclude reliance on Article 6(1)(f)

We believe that the last sentence of paragraph 114 should be reconsidered as it excludes situations where Article 6(1)(f) is treated as a general legal basis for personal data processing for marketing purposes, and consent is additionally collected for sending it via channels of communication. This is a quite common practice which is clear for users and convenient for controllers. It allows processing of data for various marketing sub-purposes (analytics, predictions, displaying etc.) but the user still is able to control his level of privacy through his/her consent to receive marketing content. Moreover, proposed exclusion of Article 6(1)(f) as a legal basis will force controllers to collect coupled consent for marketing purposes (such a consent shall cover both general marketing purposes and sending marketing content), and such a coupled consent would be a textbook example for violation of coupling prohibition (Art. 7 GDPR). Collection of two separate consents (one for general marketing purposes, second for communication of marketing) would also be unclear for users with some users clicking only on the second consent for communication without general consent for marketing purposes leading to a nonsense combination of consent. A more favourable solution would be to indicate that Article 6(1)(f) is not sufficient to be a legal basis for sending marketing communication.

Paragraph 115 seems to open the possibility that consent provided in accordance with article 5(3) ePrivacy may be compatible with a different legal basis aside from consent for the purpose of subsequent direct marketing activities, without expressly rejecting the legitimate interest. We wonder in which situation the EDPB considers compatible with the processing of personal data collected under article 5(3) ePrivacy consent for the subsequent purpose of direct marketing activities while basing such processing on legitimate interest. We come to this conclusion when it is stated "*thus normally precluding reliance on Article 6(1)(f) in this context*", as the word "*normally*" is understood to mean as "in most cases", allowing exceptions.

In relation to the previous paragraph (115) analysis, we would like to understand whether both consent and the exception to such consent in Article 13 ePrivacy Directive are directly related to consent and legitimate interest, respectively, with respect to further direct marketing communications. In other words, can we interpret the EDPB's statement to mean that the exception mentioned in Article 13 ePrivacy Directive can only be compatible with the legitimate interest with respect to the purpose of performing direct marketing activities? Or is it possible to rely on another legal basis, as suggested by paragraph 115 in relation to Article 5(3) ePrivacy Directive? We would appreciate further information on this, as well as a description of the conditions under which legitimate interest can be invoked as a valid legal basis in those scenarios.

Case-by-case assessment to be made when reliance on Article 6(1)(f) is not precluded by law

It appears problematic to equate tracking across different websites with tracking across different location devices and services (para. 120). Indeed, it may come as a surprise to data subjects that different, externally unrelated websites exchange tracking information with each other. However, if the same service is accessed from different locations or with different devices, or if it concerns analyses of different services and their use that have a close and recognisable connection with each other, such data processing is much more likely and will also not come as a surprise for data subjects. The customer even expects a unified personal experience across these services and devices. It is important to consider the individual case, for which paragraph 120 leaves however no room.

Furthermore, paragraph 120 suggests that less intrusive methods, such as sending the same commercial message to all customers who recently purchased similar products, are easier to justify. However, we find that this example does not reflect current marketing best practices, as sending repeat offers for recently purchased items is outdated and counterproductive. It might be beneficial for the Guidelines to include more relevant and realistic examples that align with modern, customer-centred marketing strategies.

We would recommend adding ad analytics and measuring engagement to the list of practices with little impact on data subjects. Additionally, since “tracking” is not defined in the GDPR – unlike “profiling” – we believe the EDPB should consider refraining from its use. It would also be useful to provide criteria to define which types of marketing might be considered intrusive, as this would play a key role in the balancing test.

3. Processing for the purpose of ensuring network and information security

The statement in paragraph 127, that “*security cannot justify an excessive processing of personal data*” suggest a restrictive approach which should be reconsidered. This requirement does not reflect the evolving nature of cybersecurity, where new security vulnerabilities and perpetrating attacks are discovered every minute. As soon as a security vulnerability has been successfully closed, criminals devise further attack scenarios, making it impossible to predict what information will be necessary and sufficient to ensure effective protection not only of these important controller interests, but also to efficiently protect the interests of business partners and customers. The requirement therefore laid down in paragraph 127 could be in contradiction with the controller's obligations under Articles 25 and 32 of the GDPR. Furthermore, data processors should still be able to fulfil their obligations under other legislation such as the Cloud Act.

4. Transmission of personal data to competent authorities

We find that paragraph 132 offers too much protection to potential criminals, as it implies that a balancing exercise should be carried out before the identification details are handed over to the authorities. We believe that it should be acknowledged that **voluntary misuse and criminal behaviour by the data subject can influence the balancing exercise**. In the past, data protection authorities have indeed taken malicious actions into account when performing the balancing exercise, and this valuable point should be reflected.

Paragraph 136 refers to a specific case where the EDPB found that, under certain circumstances, the interests or fundamental rights of the data subject could take precedence over the controller's interest in complying with a third-country law enforcement request. While this likely relates to requests under the Cloud Act, it is not stated explicitly in the Guidelines directly. Considering this to be a general guidance it puts a lot of burden and financial risk on the data controller. While companies already have policies in place to verify the authenticity and validity of such requests, as long as these points are ensured and especially in view of the threat of fines, companies should not be subject to excessively strict requirements for examining the fulfilment of such requests.