AIG RESPONSE TO THE EDPB'S GUIDELINES 1/2024 ON PROCESSING OF PERSONAL DATA BASED ON ARTICLE 6(1)(f) GDPR (8 OCTOBER 2024)

SUMMARY

1. The Advertising Information Group (AIG) welcomes the opportunity to respond to the European Data Protection Board's (EDPB) Guidelines 1/2024 on the processing of personal data based on Article 6(1)(f) GDPR. Whilst the Guidelines provide helpful clarification in certain areas, we identify several concerns requiring further consideration.

2. Guidelines on the application of the GDPR must be firmly based on the jurisprudence of the CJEU. We appreciate the EDPB's efforts to link the proposed Guidelines to relevant court cases. However, we disagree with some of the EDPB's interpretations of the relevant judgements and the application of GDPR requirements.

3. The Guidelines' requirement to assess marketing "intrusiveness" introduces problematic subjectivity beyond GDPR's established criteria. This creates undue uncertainty, particularly for SMEs, and risks driving organisations toward an overreliance on consent mechanisms—potentially overwhelming data subjects with consent requests rather than empowering them.

4. Moreover, the processing of personal data for direct marketing purposes can be based on the legitimate interest clause even if one of the communication channels used requires consent. It is important to note that direct marketing techniques are not commonly based on "extensive processing of potentially unlimited data".

5. The EDPB takes a notably stricter stance on wider public interest as a legitimate interest than other regulatory authorities, including the UK's Information Commissioner's Office (ICO). This divergence creates practical challenges for organisations operating across jurisdictions and may unnecessarily restrict activities that serve both commercial and societal interests.

6. The necessity test is based on the controller defined purpose and legitimate interest and includes a proportionality test. Reasonable expectations are just one aspect to be considered in the balancing act and do not automatically overwrite legitimate interests.

7. The Guidelines create an artificial distinction between fraud prevention and criminal offences that poses significant operational challenges. This separation risks creating unnecessary administrative burdens; discouraging private sector cooperation with law enforcement; and hampering effective public-private partnerships in combating sophisticated online advertising fraud.

8. These issues are particularly significant given advertising's essential role in financing free media, culture and sport. Digital advertising serves as a crucial tool for SMEs and charities, enabling market

AIG transparency number: 11220347045-31

access and efficient donor engagement. The Guidelines' impact must be considered against the GDPR's recognition that data protection should be balanced with other fundamental rights and freedoms enshrined in the European Charter of Fundamental Rights, including media freedom and the freedom to conduct business.

CONTEXT

9. The Advertising information Group (AIG) (transparency number: 11220347045-31) welcomes the opportunity to comment on the European Data Protection Board's (EDPB) Guidelines 1/2024 on the processing of personal data based on Article 6(1)(f) GDPR adopted in October 2024.

10. AIG is an informal pan-European network of European advertising and media associations that brings together various parts of the advertising industry: from advertising agencies, broadcaster and publisher bodies, direct marketing, to radio and online.

11. Our position on data protection is grounded in fundamental rights considerations. As noted in Recital 4 of the GDPR, the right to the protection of personal data is not an absolute right and must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. Specifically, while the Charter of Fundamental Rights protects the right to privacy and family life (Article 7) and personal data protection (Article 8) of the Charter of Fundamental Rights, it must also be weighed against Article 11(2), which safeguards media freedom and pluralism, and the freedom to conduct business (Article 16).

12. This balance is crucial as advertising and marketing are essential for the financing of free media, culture and sport. Data-driven advertising and marketing carries benefits for advertisers, service providers and users alike. We believe that data-driven advertising and direct marketing has a settled place in our society and economy as it secures fair competition and economic growth in the European Union.

13. Firstly, it facilitates users to see more timely and relevant commercial communications. This leads to a better and more personalised user experience whilst at the same time optimising consumer engagement with brands. Consumers want to be spared of advertising and marketing that is not of interest for them.

14. Secondly, businesses want to reach consumers with a potential interest in their products and services. Direct marketing techniques are designed to reconcile both the interests of consumers and business by allowing businesses to select addressees of direct marketing based on objective criteria. Numerous firms and charitable organisations depend upon direct marketing (e.g. email marketing) to promote their goods, services and initiatives. It also serves as a powerful tool for both SMEs and charities - allowing SMEs to connect with new markets and customers, whilst enabling charitable organisations to build their donor base in an efficient and scalable way.

15. The EU legislature also recognised the importance of data-based marketing by maintaining the opt-out principle in the GDPR and explicitly recognising that the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest. Hence, requiring consent for direct marketing would be disproportionate and ineffective. The use of selection criteria for direct marketing under the legitimate interest clause is possible but we also agree that it has limits. It requires a case-by-case assessment to establish whether the processing of personal data is within or outside these limits.

16. Our members demonstrate responsible practices by:
    - Not using special categories or data (Article 9) for direct marketing without the data subject's consent.
    - Not sending electronic direct marketing without consent if such a consent is required.
    - Maintaining a high degree of transparency by informing consumers in every direct marketing communication about their opportunity to object.
    - Using common marketing techniques that align with consumer expectations.

17. The effectiveness of this approach is evidenced by the limited number of complaints to data protection authorities regarding direct marketing, e.g. in Germany less than one out of 100,000 direct marketing communications leads to a complaint.

18. This submission comments on points in the guidelines that are relevant to and affect the advertising and marketing industry.

BENEFITS OF LEGITIMATE INTEREST AS A LEGAL BASIS

19. The EDPB's guidelines is welcome from the perspective that it applies the most recent CJEU jurisprudence and provides further clarity and guidance on the use of Article 6(1)(f). However, we believe that the analysis and references are incomplete.

20. The legitimate interest ground for lawful processing under Article 6(1)(f) is one the of six legal bases for processing data under GDPR. Since the implementation of GDPR, there has been an overreliance on consent, even though legitimate interest is an equally valid legal basis.

21. This legal basis is important to data controllers as it affords the flexibility to process data when it is "necessary for the purposes of the legitimate interest pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

22. We note that for processing to be based on the legitimate interest legal basis, three cumulative conditions must be fulfilled:

- First, the pursuit of a legitimate interest by the controller or by a third party;
- Second, the need to process personal data for the purposes of the legitimate interest(s) pursued (i.e., the processing of personal data must be "necessary" for those purposes); and
- Third, the interests or fundamental freedoms and rights of the concerned data subjects do not take precedence over the legitimate interest(s) of the controller or of a third party.

23. Compared with Directive 95/46/EC, the GDPR extended or clarified the scope of Article 6 (1) (f) in three ways:
    - Firstly, through Recital 47 the EU legislature cited direct marketing purposes in general as legitimate interests that may be pursued by a controller.
    - Secondly, the legislature modified the provision to include the legitimate interest of every third party and not only third parties to whom the data are disclosed.
    - Thirdly, by strengthening the transparency obligations and fairness requirements in the data subject rights, the legislature provided greater protection for the interests of the data subjects by law.

    We agree that compliance with law cannot be claimed as a mitigation measure if the requirements of the legitimate interest clause are not fulfilled. However, the greater protection provided by the GDPR impacts the weight of the interest or fundamental rights of the data subject in the first place. All three factors mean that the scope of application for the legitimate interest clause has been broadened by the GDPR, without compromising the legitimate protection of data subjects.

24. While we agree that Article 6(1)(f) GDPR cannot be considered as a legal basis "by default", there are some cases where seeking consent is neither practical nor logical. For example, when sending a reminder to a data subject that their insurance policy is due for renewal, or when processing data to prevent fraud. We believe such use-cases remain consistent with the cumulative conditions mentioned above.

25. Furthermore, legitimate interest also has an important role in promoting digital innovation. Its flexible nature, combined with organisational accountability requirements allows organisations to:
    - Adapt to new technologies whilst remaining compliant with the GDPR.
    - Improve their services and develop new data-driven solutions.
    - Maintain privacy protection.
    - Keep pace of technological advances.[1]

[1] Centre for Information Policy Leadership Whitepaper "How the legitimate interests ground for processing enables responsible data use and innovation" cipl_white_paper_-_how_the_legitimate_interests_ground_for_processing_enables_responsible_data_use_and_innovation__1_july_2021_.pdf (informationpolicycentre.com) page 11

USING LEGITIMATE INTEREST FOR THE PURPOSE OF DIRECT MARKETING: EXPECTED CLARIFICATIONS

26. The CJEU stated in C-708/18[2] in response to a specific question of the referring questing court, that the legitimate interest should be present and effective at the time of processing and not hypothetical. Hence, the wording in the Guidelines (para 14-18, 17) "*real and present*" and not "*speculative*" is not supported by the CJEU. Furthermore, it should be clarified that since C-26/22 and C-64/22[3], the requirement that the legitimate interest should be present and effective, and not hypothetical at the time of processing[4] is no longer considered by the CJEU in the first step of the test but as part of the necessity test.

27. Other inaccuracies should also be revised. Example 3 (para 18) described in the Guidelines links to judgement C-708/18 in which the CJEU confirmed that the legitimate interest must be present and effective as at the date of the data processing and must not be hypothetical at that date. As mentioned earlier, the CJEU did not include this criterion as part of the first test, but even if this criterion was applied, the CJEU made clear in C-26/22 and C-64/22 that the collection of data for potential requests from (not yet identified) third parties can constitute a legitimate interest. Thus, the CJEU makes clear in its judgement that the threshold for determining the existence of a legitimate interest is low.

28. Furthermore, the first step of the test asks simply whether a legitimate interest exists. This implies that a legitimate interest would have to be so hypothetical that its weight and consideration is zero. This is almost never the case and certainly would not apply in Example 3. In that example, the purpose of the data collection is to build a database for potential marketing activities. We argue that the database has economic value because it would enable the publisher to market a new publication, and the purpose of creating economic value is itself a legitimate interest. It is not relevant whether the publication is already scheduled. The publisher has launched publications in the past and it would not be unexpected for a publisher to launch new publications. This reasoning alone is sufficient given that the CJEU accepted in C-26/22 and C64/22 that a potential use can justify a legitimate interest. Therefore, we would argue that the purpose to build the database is based on a present and effective legitimate interest and not hypothetical.

29. As with C-26/22 and C-64/22, the question is essentially whether the potential use in the future is sufficient as part of the necessity test, and potentially within the balancing process. In Example 3 the processing would be necessary, because the publisher would not be able to collect the specific addresses at a later point. The potential customers would otherwise be lost for the marketing

[2] https://curia.europa.eu/juris/document/document.jsf?text=&docid=221465&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=7890042

[3] Schufa Holding, Joined Cases C-26/22 and C-64/22 (CJEU - C-26/22 SCHUFA Holding 7 Dec 2023 (dpcuria.eu))

[4] C-708/18, para 44

campaign for a new publication. Approaching former or existing customers is a very common and effective marketing technique. This legitimate interest would not be outweighed by data subject interests, because the legitimate interest has substantial commercial weight and the impact to the data subject would be minimal.

30. We further note that the EDPB guidance suggests that controllers ought to consider the level of intrusiveness of their chosen marketing practice when conducting the legitimate interest balancing test (para 114, 120). We think that this is problematic for several reasons.

31. Firstly, we contest the conflation of advertising and marketing. While marketing and advertising are often confused or used interchangeably, marketing is the broader discipline that encompasses all activities involved in bringing a product or service to market. It includes initial market research and product development, to pricing strategies, distribution planning, brand development, customer relationship management, and analysing performance metrics.

32. Advertising, on the other hand, is just one component of the larger marketing framework. It specifically refers to paid promotional activities through various media channels, such as television, radio, print media, digital platforms, out of home, and social media advertisements.

33. Secondly, given that this goes beyond the legitimate interest cumulative conditions, it therefore warrants further explanation as to why marketing should be assessed at a higher standard vis-à-vis other activities, considering that Recital 47 of the GDPR states that the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest of the controller. We therefore believe that just as the lawfulness of the processing of data as such does not depend on a marketing communication channel being lawful or unlawful (unlike Example 2 in the Guidelines), the reliance on Article 6 (1) (f) GDPR should not be excluded because provisions on the (subsequent) use of certain marketing channels require the user's consent for this.

34. Furthermore, direct marketing falls within the scope of Article 13(2) of Directive 2002/58/EC ("ePrivacy Directive"). Given the *lex-generalis-lex specialis* relationship between the GDPR and the ePrivacy Directive, it is important to recall that Article 95 of the GDPR provides that the regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the EU, in relation to matters for which they are subject to specific obligations with the same objective set out in the ePrivacy Directive.

35. Thirdly, considering the level of intrusiveness appears to be a subjective test – one person's level of intrusiveness will be different to another person. This subjectiveness would likely lead to many businesses feeling uncertain over the use of legitimate interest as a legal basis. Instead of maintaining the balance and equal footing across the six legal bases, we argue that this would drive

further reliance on consent. While consent might be viewed as the gold standard, we argue that data subjects being inundated with consent requests does not empower the data subject. Instead, it impairs the data subject from making informed and rational choices about the consent choices they are making.[5]

36. Given the additional legal uncertainty, this would likely have a higher impact on SMEs, which make up 99% of business in the EU,[6] because in many cases they do not have the legal resources to assist them in navigating complex regulatory frameworks.

37. Fourthly, although the Guidelines reference the Meta v. *Bundeskartellamt case*, it cannot be cited as evidence for the EDPB's opinion. The Meta v. *Bundeskartellamt case* was very specific in that it related to Meta's practice of large-scale collection of off-Facebook user data for online data processing.[7]

    "The processing at issue in the main proceedings is particularly extensive since it relates to ***potentially unlimited data*** *and has a significant impact on the user,* ***a large part – if not almost all – of whose online activities are monitored****"*

38. Common direct marketing practices are not based on "*extensive processing of potentially unlimited data*". For the remainder, the expectation is to be asked for consent for online-tracking. This follows the requirement under the ePrivacy Directive. However, data processing for direct marketing techniques do not fall under the application of the ePrivacy Directive but under the opt-out regime of the GDPR.

39. Hence, we caution against interpreting the CJEU's judgement more widely to general marketing practices.

WIDER COMMUNITY AND WIDER PUBLIC INTEREST AS A LEGITIMATE INTEREST

40. We note that the EDPB guidance takes a notably broader and, in some respects, a stricter stance on public interest considerations (Paragraph 25).

41. Firstly, it would be appropriate and helpful to further elaborate on the findings of C-621/22 which confirms the wide scope of legitimate interest in relation to commercial interests. Taking the history of the legitimate interest clause into account, any third-party interest can provide weight in the legitimate interest clause. As the CJEU stated in C-26/22 and C64/22, these third parties do not have

[5] https://harvardlawreview.org/print/vol-126/introduction-privacy-self-management-and-the-consent-dilemma/
[6] Annual report on European SMEs 2022/2023. https://op.europa.eu/en/publication-detail/-/publication/12f499c0-461d-11ee-92e3-01aa75ed71a1/language-en
[7] Ibid. para 118

to be specified. This joint case also shows that wider community interests do count. If a company processes address data and selection criteria to allow potential other companies to send out direct marketing material, the legitimate interest of these potential advertising companies provides weight. As there have been some divergent views on this from data protection supervisory authorities in the past, we ask that the legal situation established by the CJEU be presented more clearly (para 25).

42. Secondly, according to the EDPB, broader public interests should primarily be handled under Article 6(1)(e) or (c) of the GDPR, whilst Article 6(1)(f) should be limited to the legitimate interest of specific controllers or third parties. Controllers must demonstrate that any additional activities beyond legal obligations serve their own legitimate interest or those of specific third parties, rather than wider societal benefits.

43. This is based on the interpretation of the Meta v. *Bundeskartellamt* case where the CJEU stated (para 124):

[…] relating to the sharing of information with law-enforcement agencies in order to prevent, detect and prosecute criminal offences, it must be held that that objective is not capable, in principle, of constituting a legitimate interest pursued by the controller, within the meaning of point (f) of the first subparagraph of Article 6(1) of the GDPR. A private operator such as Meta Platforms Ireland cannot rely on such a legitimate interest, which is unrelated to its economic and commercial activity. Conversely, that objective may justify processing by such an operator where it is objectively necessary for compliance with a legal obligation to which that operator is subject.

44. However, we believe the correct way to interpret the CJEU's opinion is that law enforcement objectives cannot constitute a legitimate interest under Article 6(1)(f). Private operators (like Meta) cannot routinely claim law enforcement as a legitimate interest as it is unrelated to their business.

45. In contrast to the EDPB's position, it is worth noting that the ICO adopts a more flexible approach, suggesting that general public interest can strengthen a controller's position when balancing interests against individual rights under Article 6(1)(f).[8]

46. Where these differences may manifest is when a controller processes data for fraud prevention. The ICO might consider the broader public benefit of reducing financial crime, while the EDPB only appears to focus on the controller's specific interest in protecting their business.

47. There is also a marked difference in how 'necessity' is interpreted. The EDPB emphasises strict necessity, whilst the ICO – along with other CJEU cases (see C-26/22 and C64/22) requires only that

[8] See also, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/legitimate-interests/

processing be targeted and proportionate to achieve its purpose. This aligns with established UK case law, notably the South Lanarkshire Council v Scottish Information Commissioner case of 2013, which confirmed that 'necessary' should be interpreted as 'reasonably necessary' rather than 'strictly necessary' when considering legitimate interest.[9]

RELYING ON LEGITIMATE INTEREST TO PREVENT, DETECT AND PROSECUTE CRIMINAL OFFENCES

48. Combatting fraud in the online advertising ecosystem is a major challenge for legitimate advertisers, publishers, ad platforms, as well as raising important considerations for data subjects' rights. Online advertising fraud employs sophisticated techniques such as cloaking, where malicious advertising is disguised as legitimate campaigns. The complexity of these deceptive practices necessitates analysis of multiple signals to detect malicious activity, making fraud detection particularly challenging.

49. Under Article 6(1)(f) GDPR and as explicitly mentioned in Recital 47, fraud prevention activities can be based on legitimate interest. While the EDPB guidelines (para 102) note there is no formal definition of "fraud prevention", the prevention of online advertising fraud logically falls within this scope, given its direct relationship to commercial activities.

50. Furthermore, preventing and tackling fraud is an integral part of a data controller's commercial and economic interest and can coincide with a public interest. This was reflected in the Data Protection Working Party 29's 2014 Opinion[10]:

    "It can also be the case that a private business interest of a company coincides with a public interest to some degree. This may happen, for example, with regard to combatting financial fraud or other fraudulent use of services. A service provider may have a legitimate business interest in ensuring that its customers will not misuse the service (or will not be able to obtain services without payment), while at the same time, the customers of the company, taxpayers, and the public at large also have a legitimate interest in ensuring that fraudulent activities are discouraged and detected when they occur".

51. The EDPB interpretation (para 131) of Meta v. *Bundeskartellamt* creates a distinction for criminal offences and sets out that private businesses generally cannot rely on legitimate interest for collecting and sharing data with law enforcement, as crime prevention is considered "unrelated to economic and commercial activity" of private businesses. Such information sharing must be based on a legal obligation (Article 6(1)(c)).

---

[9] UK Supreme Court (2013). South Lanarkshire Council (Appellant) v The Scottish Information Commissioner (Respondent) (Scotland). https://www.supremecourt.uk/cases/docs/uksc-2012-0126-judgment.pdf. Para 27.

[10] Data Protection Working Party 29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014, III.3.4 (a)(ii) pg 35 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

52. Somewhat confusingly, the EDPB also states that legitimate interest can indeed be invoked (para 132) and the controller could consider relying on Article 6(1)(f) GDPR to share information on any possible criminal acts or threats it may occasionally become aware of with law enforcement authorities so long as the controller does not collect and store personal data in a preventive and systematic manner specifically to be able to provide such data to law enforcement authorities.

53. This aligns with Recital 50 of the GDPR, which states that legitimate interest **may be** relied on for the purposes of:

    "[…] *Indicating possible criminal acts or threats to public security and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal acts or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller."*

54. Note that there is no mention of collection and storage personal data in a preventive and systematic manner specifically to be able to provide such data to law enforcement authorities.

55. In any case, this apparent distinction between fraud prevention and criminal offences creates a practical challenge for addressing online advertising fraud. It would mean that commercial organisations must carefully structure their anti-fraud programs to separate commercial fraud prevention (where legitimate interest might apply) from criminal law enforcement cooperation (which would appear to require a different legal basis). Furthermore, they would need to establish clear thresholds for when fraud prevention becomes a criminal matter and implement strict data minimisation practices.

56. For example, using data analysis to prevent click fraud or invalid traffic might fall under legitimate interest, but systematically collecting this data to report potential criminal activities to law enforcement would not. Commercial organisations must therefore carefully scope their fraud prevention measures to be proportional and directly related to their business operations, while having separate procedures for handling potential criminal matters.

57. We argue that this creates unnecessary administrative burdens and disincentivises companies from sharing data with law enforcement. While, companies may become better at detecting fraud, fundamentally it does not address the criminality of those perpetuating fraud who will adapt their techniques accordingly such that it becomes persistent pattern of cat and mouse. The EDPB's position potentially hampers public-private partnerships that have proven valuable in providing intelligence for law enforcement to identify and disrupt criminal activity.

REGARDING DIRECT MARKETING: FURTHER EXPLANATIONS ON NECESSITY NEEDED

58. As mentioned above, the necessity test according to the CJEU requires that the legitimate interest pursued cannot "*reasonably*" be achieved just as effective by other means less restrictive of the fundamental rights and freedoms of data subjects. We notice that the necessity requirement also covers the data minimisation requirement. Additionally, it overlaps with the storage limitation principle. If, and so long as the necessity requirement is fulfilled, these principles are not breached.

59. The necessity test has two limitations. Firstly, the purpose of the processing is not to be questioned as such. For example, if a controller decides to use direct marketing techniques, the question is not whether this type of marketing is necessary to successfully run the company. The management chooses the purpose of the processing. The necessity test accepts the decision and asks whether that purpose can be otherwise achieved with less impact on the data subject. Secondly, the necessity test includes a proportionality requirement ("*reasonably*"). It is not required that the controller uses less impactful alternatives whatever they cost. For example, one could argue that the processing of selection criteria is not necessary because the controller can send the marketing communication to all contacts. However, this would be very expensive and ineffective, and therefore, it would not be reasonable. It would be helpful to highlight the limits of the test and the proportionality requirement, because the necessity requirement is sometimes misunderstood.

FURTHER EXPLANATIONS ON BALANCING NEEDED

60. We agree that the balancing test is an objective test. The test aims to protect the data subjects. In consumer protection law, the CJEU applies such tests to the "*average*" consumers (for example in C-611/14). The same should apply for the legitimate interest test, because the purpose of Article 21 (1) GDPR is to consider the "particular situation" of a data subject. Hence, Article 21 GDPR would have no role if the legitimate interest test already takes the particular situation of the data subject into account.

61. The draft Guidelines explain the application of the criterion of reasonable expectations. It should be noted, however, that this is not an independent criterion in the legitimate interest clause. Recital 47 of the GDPR states that whilst data subjects' reasonable expectations could override a controller's interests, this *per se* does not necessarily lead to "a lack of reasonable expectations" being automatically prohibited. The EDPB's guidelines emphasise the important role of reasonable expectations in the balancing test. However, reasonable expectations should only be considered *inter alia* risks against individual interests and fundamental rights, otherwise there is the potential to unduly restrict processing based on legitimate interests.

62. The Guidelines also suggest that reasonable expectations should be considered independently of information provided to data subjects (para 53). However, this appears to overlook how transparency obligations under Articles 12-14 GDPR are crucial in shaping expectations and empowering individuals. Transparency ensures fair and lawful processing whilst helping align data

subjects' expectations with provided information. Downplaying the role of transparency could undermine the principles of the GDPR, as informed data subjects better understand controllers' practices. Also, as a point of principle recital text is not legally binding, nor can it override the operative text. Furthermore, there should be a "purposive" interpretation to the recitals, rather than a strict literal approach. In other words, if the text is not clear, the recitals can be interpreted to give effect to the aim or spirit of the legislation, considering its context and general objectives.

TRANSPARENCY

63. In addition, we believe that it is necessary for the EDPB to evidence how enhanced transparency measures beyond GDPR requirements, such as publishing balancing tests, would influence reasonable expectations and foster trust. Whilst common practices do not automatically align with expectations, their prevalence can shape what individuals reasonably anticipate. Reasonable expectations should be assessed contextually taking into consideration the level of transparency, the nature of the service, and the context in which the data was collected.

64. We agree that the controllers should inform data subjects about the legitimate interests pursued. Under the GDPR, the obligation to inform data subjects about the legitimate interests pursued is strict under Article 13. Under Article 14, controllers only need to provide information "necessary to ensure fair and transparent processing", and not required at all under Article 15. It is not correct to interpret Article 5 (2) as a data subject right. The obligation to demonstrate compliance does not create a right for the data subject to get access to the underlying documentation. There is also no right of the data subjects to receive the records of data processing activities under Article 30 or the documentation of data protection impact assessments under Article 35. The access right of the data subject is exclusively regulated in Article 15.

CONCLUSION

65. The EDPB's Guidelines on Article 6(1)(f) GDPR provide welcome clarity in several areas but also raise several concerns for the advertising industry and warrant further consideration.

66. First, the guidelines' approach to marketing activities introduces unnecessary complexity by requiring assessment of "intrusiveness" - a subjective criterion that goes beyond the GDPR's cumulative conditions for legitimate interest. This creates legal uncertainty, particularly for SMEs, and risks driving further reliance on consent mechanisms that may ultimately diminish rather than enhance data subject empowerment.

67. Second, the EDPB's stricter interpretation of public interest considerations compared to other regulatory authorities (such as the ICO) creates practical challenges. The narrow interpretation of the Meta v. *Bundeskartellamt* ruling could unnecessarily restrict legitimate business activities that serve both commercial and broader societal interests.

68. Third, the distinction between fraud prevention and criminal offenses, creates operational challenges that may impede effective cooperation between private sector organisations and law enforcement. This could ultimately undermine efforts to combat sophisticated online advertising fraud and other digital threats.

69. Fourth, the Guidelines should, as stated above, reflect the current case law of the CJEU with regard to the legitimate interest, necessity and the balancing test more accurately and completely, as this would be conducive to legal certainty and the application of the GDPR in accordance with fundamental rights.

70. We therefore recommend that the EDPB:
    - Reconsider its position on assessing marketing intrusiveness.
    - Provide clearer guidance on the distinction between systematic and occasional sharing of information with law enforcement.
    - Develop more practical frameworks for balancing commercial fraud prevention with criminal law enforcement cooperation.
    - Consider alignment with other regulatory approaches to reduce fragmentation in the digital single market.
    - Acknowledge that the necessity test is based on the controller defined purpose and legitimate interest and includes a proportionality test.
    - Reflect that reasonable expectations are just one aspect to be in the balancing act and do not automatically overwrite legitimate interests.

71. These adjustments would help ensure that the guidelines support both effective data protection and the legitimate operational needs of the advertising industry, while maintaining the careful balance envisioned by the GDPR between protecting individual rights and enabling responsible data processing for legitimate business purposes.

Advertising Information Group

20 November 2024