EDPG Guidelines on legitimate interest

Overarching Feedback

The EDPB Guidelines fail to recognise the potential of Article 6(1)(f) GDPR and therefore restrict its scope of application to an unacceptable degree. Article 6(1)(f) GDPR is wrongly consigned to a shadowy existence, even though it has the potential to be a central standard for data processing operations and to enable a fair balance of interests. By unnecessarily restricting the legal basis at various points in the Guidelines, the EDPB is depriving it of the opportunity to fulfil its potential and to achieve a fair balance between all fundamental rights, freedoms and principles in line with the principle of proportionality, which reflects the social function of data protection. This necessity is emphasised at a central point in the General Data Protection Regulation in Article 1(3) GDPR and in explicit terms in Recital 4. In order to fully exploit the possibilities offered by Article 6(1)(f) of the GDPR, a broad interpretation rather than an unnecessarily narrow reading of the norm would be more appropriate. Article 6(1)(f) GDPR is a good and appropriate legal basis, and it must be possible to use it effectively in the corresponding manner.

Individual Feedback

Key statement within the Guidelines	**Input to be included when answering the public consultation**
Executive Summary	
Article 6 (1)(f) GDPR should **not** be treated as a "**last resort**" (ExecSum)	This is a meaningful clarification. In general the Guidelines should highlight the potential and importance of Article 6(1)(f) GDPR and the necessity to apply the principle of proportionality when interpreting the requirements of Article 6(1)(f) GDPR to ensure that a balance with all fundamental rights, freedoms and principles can be achieved.
Interests in the sense of Article 6 (1)(f) GDPR **must be lawful, precisely articulated and present.** (ExecSum)	The requirements of precisely articulated and present interests don't have a legal basis in the GDPR. The necessity of precisely

Key statement within the Guidelines	Input to be included when answering the public consultation
	articulated interests refers to the information obligation in Article 13(1)(d) GDPR. However, information obligations are to be considered separately. With respect to the necessity of a “present interest” it should be considered that if a future use case can be predicted with certainty the interest to pursue this should not be excluded from being qualified as legitimate from the outset.
The balancing of opposing interests and rights should be focused on the following factors: ● **Nature and source of the legitimate interest** ● Impact of the processing on the data subject ● Reasonable expectations ● Existence of additional safeguards (ExecSum)	The term “source” is a new term not explained in the Guidelines and hence creating unclear obligations for the data controller.
Introduction	
GDPR does **not** establish any **hierarchy between the different legal bases** laid down in Article 6(1) (para. 1)	This a meaningful clarification which highlights that Article 6(1)(f) GDPR is neither a less valid nor less important legal basis in comparison to other legal bases like consent.
The **balancing exercise** must be performed **for each processing** before it is carried out (para. 7)	This adds to our impression that EDPB wants to make it particularly complicated and not a scalable process at all the rely on Article 6(1)(f) GDPR because the requirements which are defined here are so granular and a differentiation and sub-division has to be considered for so many cases that a meaningful assessment to permit a number of use cases cannot be done anymore. We think that it actually also contradicts the whole sense of Article 21 GDPR which states that if your individual situation should differ from what is normally expected, you can object. That means that the GDPR itself assumes that normally, assessments are made based on broader assumptions and not based on an assessment for every individual
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)	

Key statement within the Guidelines	Input to be included when answering the public consultation
	data subject. Furthermore it has to be considered that the legitimate interest assessment has to take place before a data processing operation can take place. At this point in time a data controller normally has no absolute clarity regarding the data subjects and their particularities. Hence, this interpretation ignores the chronology of legal considerations and controllers information at different points in time.
Applicability of Article 6(1)(f) GDPR as a legal basis	
The LIA should be made with the **involvement of the DPO** and should be documented (para. 12)	There is no legal basis for this requirement in the GDPR.
A **wide range of interests** is, in principle, capable of being regarded as legitimate, such as having **access to information** online, **ensuring the continued functioning of publicly accessible websites**, obtaining the personal information of a person who damaged someone's property in order to sue that person for damages, protecting the property, health and life of the co-owners of a building, **product improvement**, and **assessing the creditworthiness of individuals**, among others (para. 16)	It is appreciated that in general a wide range of interests is considered legitimate.
Analysis of the necessity of the processing to pursue the legitimate interests	
It is about assessing that the interests pursued **cannot reasonably be achieved just as effectively by other means less restrictive** of the fundamental rights and freedoms of data subjects. The condition relating to the need for processing must be examined	The data minimisation requirement 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.

Key statement within the Guidelines	Input to be included when answering the public consultation
in conjunction with the "data minimisation" principle (para. 29)	
Methodology for the balancing exercise	
The purpose of the balancing exercise is **not to avoid any impact** (para. 33)	This is a useful clarification that should be borne in mind when imposing more and more restrictions on data controllers.
Affected interests can be **financial interests, social interests or personal interests** (para. 38)	GDPR mostly puts obligations on companies and not on private persons because for them there is an exceptional clause and then the interests mentioned here are almost purely interests of an individual or an NGO. The only interest EDPB assumes to be pursued by a company is a financial interest but this puts already a negative perspective on that and it doesn't reflect reality because indeed we are also pursuing the goal of improving our services for our customers and to minimise environmental impact by strictly adhering to our privacy and sustainability principles just to name a few of them.
When assessing the impact on the data subject **positive and negative effects should be considered** (para. 39)	More guidance on possible positive impacts would be desirable as the Guidelines only mention the relevance of positive effects once and don't elaborate on this point or give examples. [Maybe we don't ask for more guidance but] we present what we would consider good examples ● 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 ● Improve size recommendations and fit predictors ● Improving the customer care service ● Improve customer journeys

Key statement within the Guidelines	Input to be included when answering the public consultation
Further **consequences of the processing** to be considered are: ● Potential future decisions or actions taken by third parties ● Production of legal effects ● Exclusion or discrimination ● Defamation ● Financial losses ● Exclusion from a service without real alternative ● Risk to freedom, safety, physical and mental integrity (para 45)	The list of criterias shows that positive consequences are not considered sufficiently yet and there is no elaboration or examples given for positive effects. This would be desirable and it would be interesting to hear whether the examples given above could serve (see above).
Broader emotional impacts from a data subject losing control over personal information should be considered as well. For example, continuous online monitoring of online activities by a platform may give rise to the feeling that a data subject's private life is being continuously observed. (para. 46)	This should be corrected and linked to a specific right or interest to avoid misuse and misunderstandings regarding this argument. Furthermore it highlights that this is actually a digital fairness topic which is mixed up with GDPR considerations and forced into this guidance.
Regarding the data subject's reasonable expectations: the f**act 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)	This is not convincing at all. It goes without saying that a common practice for a specific business sector that is known by the customers influences their expectations. Furthermore it should be taken into consideration that this is a process in motion. Data processing operations that might have been little known and little expected in 2018 might nowadays be very well known and expected by customers requesting a specific service.
The omission of information can contribute to the data subject being surprised of a certain processing, **the mere fulfilment of the information obligations is not sufficient in itself to consider that the data subject can reasonably expect a given processing**.	It is not convincing at all to consider the lack of information relevant for the expectations of a data subject but the presence of information not. This is cherry picking at the expense of the data controller and illustrates the unreasonable restrictive approach of the EDPB.
However, it should be noted that **contractual provisions** regarding personal data **may have a bearing on the reasonable**	The impact of contractual provisions on a data subject's reasonable expectations can only play a role if data processing is at the core of

Key statement within the Guidelines	Input to be included when answering the public consultation
expectations of data subjects (footnote 61)	the contract fulfilment and therefore there is a need to include data processing provisions in contractual provisions. In these cases a data controller will not rely on Article 6(1)(f) but 6(1)(b). In Article 6(1)(f) cases a contract is not the place to include data processing provisions but a Privacy Notice is the place where that information would be expected. That's why it doesn't make sense to grant a higher importance to information in a contract within an Article 6(1)(f) GDPR context. This gives the impression that requirements of different legal bases are mixed here and a tendency is present to let data protection considerations rule over civil law.
Contextual elements to be considered for the balancing of interests are: ● Existence of a relationship with the data subject (distinguish between customers and non-customers) ● Proximity of the relationship (is there a relationship with the controller or only with someone in the controllers group structure) ● Place and context of the data collection (CCTV in sauna unexpected but in a bank) ● Nature and characteristics of the service (regular customer vs. mere prospective customer) ● Legal requirements (applicability of confidentiality requirements) (para. 54)	In view of the relevance of the proximity of the data controller to the data subject, it is understandable that completely different services that present themselves to the data subject as completely different but are offered by one and the same controller or under its responsibility should be taken into account with regard to the expectations of the data subject. This strict distinction between the company of a group with which the data subject has a contractual relationship and other companies of this group that process the data subject's data is not appropriate, however, where the data subject is clearly offered coherent services with different features that are the responsibility of a single company group. [This statement is pretty obviously directed at Meta and its very different offers: Facebook, Instagram, WhatsApp… but the rule should be applied more differentiated]
Regarding the **reasonable expectations of an average data** subject it should be taken into account ● The age ● Whether data subject is a public figure ● The data subject's professional position and the level of understanding and knowledge	With regard to the requirements set out here, it also follows from the existence of Article 21 GDPR that the general considerations of the balancing of interests must be based on generalised considerations and 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. Furthermore,

Key statement within the Guidelines	Input to be included when answering the public consultation
(para. 54)	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. For reasons of data economy, data controllers often do not have such information at all.
Mitigation measures that the **controller is** legally **obliged to implement cannot speak in favour** of its interest. For that reason, **mitigating measures can, for instance, not consist of measures meant to ensure** compliance with the controllers' information obligations, security obligations, obligations **to comply with the principle of data minimisation**, or the fulfilment of data subject rights under the GDPR, and must go beyond what is already necessary to comply with these legal obligations under the GDPR. (para. 57)	It goes without saying that 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, data controllers who limit data processing to less data than would be justified for a particular use case should be rewarded with a positive assessment of this restrictive decision.
Relationship between Article 6 (1)(f) GDPR and data subjects rights	
In any case, information to the **data subjects** should make it clear that they **can obtain information on the balancing test upon request**. (para. 68)	There is no legal basis for this in GDPR.
If a data subject objects according to Article 21 GDPR but doesn't elaborate much on its particular situation the request cannot be dismissed but the **controller may ask the data subject to specify the request**. (para. 71)	This has no legal basis in the GDPR.
Contextual application of Article 6 (1)(f) GDPR	

Key statement within the Guidelines	Input to be included when answering the public consultation
Processing for the purpose of preventing fraud	
Recital 47 clarifies that processing of personal data strictly necessary for the purpose of **preventing fraud may constitute a legitimate interest** of the controller. (para. 100) The **detection of fraud can**, in principle, **also be considered to be covered**. This seems to be the only way to carry out the necessary analysis of weaknesses in order to prevent further fraud (para. 102)	Recital 47 clarifies that processing of personal data strictly necessary for the purpose of preventing fraud also constitutes a legitimate interest of the data controller concerned. Thus, recital 47 doesn't state that fraud prevention "may constitute" a legitimate interest but that it "constitutes" one.
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, as well as other third parties, may also have a legitimate interest** in ensuring that fraudulent activities are discouraged and detected when they occur. (para. 103)	It is appreciated that it is acknowledged that certain interests don't only serve the data controller but its partners and customers as well such as fraud prevention, prevention of a misuse of services but even prevention of obtaining services without payment.
To outweigh the data subject's interests the **data** to be processed **must be accurate and** demonstrably **relevant to prevent fraud of substantial importance**. (para. 105)	These findings unduly restrict the data controller in such an important business process as fraud prevention. It has just been emphasised that this is not only in the interest of the controller, but equally in the interest of its partners and the data subject itself. Accordingly, the necessary data processing operations should be legitimised to a large extent. This is particularly true in the context of criminal processes being in a constant state of flux: as soon as the data controller has found a way to close a gateway for criminal activity, the attackers will work to find a new gateway. It is therefore almost impossible to predict which data processing operations will be necessary to effectively combat crime and to prevent harm to the data controller, his business partners and, above all, the customers.

Key statement within the Guidelines	Input to be included when answering the public consultation
Processing for direct marketing purposes	
Case-by-case assessment to be made when reliance on Article 6(1)(f) is not precluded by law	
Certain marketing practices can be considered intrusive from the perspective of the data subject, notably if they are based on extensive processing of potentially unlimited data. For example, the balancing test would hardly yield positive results for **intrusive profiling and tracking practices** for marketing purposes, for example those that involve tracking individuals **across multiple websites, locations, devices and services**. (para. 120)	[This statement also seems to be very much geared towards Meta and its practice of tracking across all services in the past]. It seems problematic to equate tracking across different websites with tracking across different location devices and services. 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. It is important to consider the individual case in this regard but the statement leaves very little room for individual considerations here. This is another example of how Article 6(1)(f) GDPR fails in its interpretation by the EDPB to serve for a balanced and proportionate assessment.
Less intrusive methods are easier to justify e. g. sending the same commercial communication to all existing customers who have already bought products similar to those that are advertised (para. 120)	We all know that the last thing I need just after I bought a new winter jacket is a winter jacket. This super antique and annoying and inefficient marketing recommendation should not be included in Guidelines anymore but should be reflected critically and replaced by more meaningful and realistic examples.
The right to object to processing for direct marketing	
Processing for the purpose of ensuring network and information security	

Key statement within the Guidelines	Input to be included when answering the public consultation
Security cannot justify an excessive processing of personal data (para. 127)	This is also a hint towards a very restrictive approach of the EDPB which is to be criticised. Furthermore, this requirement ignores the reality that new ways and means of detecting security vulnerabilities and perpetrating attacks are discovered every minute. As soon as a security vulnerability has been successfully closed, criminals devise further attack scenarios. It is therefore not possible 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 has the potential to establish a contradiction with the controller's obligations under Articles 25 and 32 of the GDPR.
When a controller is victim of a cyber-attack the **IP addresses** and online identifiers **of perpetrators should only be shared with law enforcement authorities if the interest** to indicate possible criminal acts or threats to public security **is not outweigh** by the interest and rights and freedoms of the data subject concerned (para. 132)	It seems a very strict approach to protect perpetrators in this context and it should at least be mentioned how a voluntary misusing and criminal behaviour by the data subject can influence the balancing exercise. In the past, data protection authorities took malicious actions into account when performing the balancing exercise. This important point is not addressed here.
It can be noted that the EDPB, in a specific situation, has previously taken the view that the **interests or fundamental rights and freedoms of the data subject**, under those particular circumstances, **would override the controller's interest in complying with a request from a third country law enforcement authority** in order to avoid sanctions for non-compliance. (para. 136)	The case refers to requests under the Cloud Act but this is not stated explicitly in the text itself. Considering this to be a general guidance it puts a lot of burden and financial risk on the data controller. It goes without saying that companies have policies in place for verifying the authenticity and validity of requests, but 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.