

20 November 2024

AmCham Romania’s Proposals for EDPB’s Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR

#	PARA.	CURRENT TEXT	OBSERVATIONS/PROPOSALS
1	9	Article 6(1)(f) GDPR cannot be considered as a legal basis “by default”. On the contrary, before relying on such a legal basis, the controller should perform a careful assessment of the planned processing and follow a specific methodology.	<p>OBSERVATION: In this context we consider that the terminology used is not the most fortunate, as it can make one conclude that a special methodology is needed prior to choosing the legal basis of legitimate interest, which could be translated into a different Procedure of how to choose the lawful basis. Our recommendation is that a wording such as: „The Data Controller should conduct an analysis on choosing the appropriate lawful basis and not choose by default legitimate interest” is more appropriate, as usually such an analysis is conducted by a legal team and choosing the lawful basis based also on national legislation cannot really translate into or be standardized through a methodology, as law interpretation is somewhat nuanced.</p> <p>PROPOSAL: Article 6(1)(f) GDPR cannot be considered as a legal basis “by default”. Choosing the lawful basis for a certain processing activity should be the result of a careful analysis off all available lawful basis available to art. 6 GDPR and the appropriate lawful basis should be selected. If legitimate interest is chosen, it must be supported by a documented Legitimate Interest Assessment to demonstrate that the interest is adequate, the processing is not overly intrusive, and the balancing test has been met. Moreover, the decision-making process for any legal basis should be properly documented to ensure compliance and transparency.</p>

2	20	<p>However, the reference to an interest pursued by “a third party” in the wording of Article 6(1)(f) GDPR indicates that the interest(s) of one or more specific third parties may be legitimately pursued within the meaning of Article 6(1)(f),³² and may thus be balanced against the interests or fundamental rights and freedoms of the data subject.³³ In some cases, the processing of personal data may serve to pursue simultaneously the legitimate interests of the controller and of a third party.³⁴ The legitimate nature of the interest of a third party must be assessed following the same criteria which apply with respect to the controller’s own interests.</p>	<p>OBSERVATION: More clarity is needed when discussing a legitimate interest of a third party. Throughout the Guidelines the idea arising is that the original Controller needs to make the assessment if certain data can be processed by a third party based on their legitimate interest and also by conducting the balancing test. It is not lawful for a Controller to assess if a different Controller (third party) has the legitimate interest to process certain data, and more so the original Controller does not have all the information to conduct a balancing test on behalf of the third party. In such a case, it would mean that an entity established the lawful basis for a completely different entity without being in a relationship of Controller-Processor that would allow such control. Based on the present wording, this provision is nearly unapplicable as no Controller will take responsibility from a privacy standpoint and for conducting a balancing test for another entity with whom they share no relation.</p> <p>PROPOSAL: (...)The legitimate nature of the interest of a third party must be assessed by that third party following the same criteria which apply with respect to the controller’s own interests and presented to the Controller in order for the latter to be able to prove that the processing made for a third party was lawful. In such cases, the Controller should consider why the third party wants the information, whether they actually need it, and what they will do with it. While the Controller must demonstrate that the disclosure is justified, it will be the responsibility of the third party to determine and document the lawful basis for their own subsequent processing.</p>
3	23	<p><i>Disclosure of data for purposes of transparency and accountability.</i> One important context where a legitimate interest of a third party may be identified is the case of disclosure of data for purposes of transparency and accountability (e.g., in certain circumstances, the disclosure of the salaries of the top management in a company), where this is not mandated by law or contract. In this context, it can be considered that the disclosure is done primarily not in the interest of the controller who discloses the data, but</p>	<p>OBSERVATION: Due to the specificity of processing data in the legitimate interest of a third party, specific applicable examples would be more helpful in understanding the applicability of this provision. It was mentioned above in the example with the neighborhood watch that installing video surveillance to monitor possible criminal activities in the area was very vague and general and therefore not specific and couldn’t mean that processing would be carried out based on legitimate interest. Nonetheless, in para. 23 it is mentioned that disclosure of salaries in the name of transparency and accountability is a valid legitimate interest, although in this case we do not have a specific purpose and moreover, disclosing certain data in the name of transparency/accountability</p>

	<p>rather, in the interest of the recipients of this information, such as the employees or the shareholders of the company.</p>	<p>will create a pathway of breaching confidentiality by abusing the legitimate interest of a third party for knowing certain information (e.g. breach of salary confidentiality for the top management or any other employee). Such disclosure of personal data in the legitimate interest of a third party, aside from requiring a clarified mechanism (Who makes the assessment of the legitimate interest? Is the Controller making the disclosure mandated to disclose the data although the legitimate interest presented is not in their opinion legitimate? etc.), should be made only in relation with activities that are investigated by public authorities in order to prevent abuse and breach of confidentiality of personal data of certain individuals in the name of a third party's legitimate interest. Otherwise, every employee could ask in the name of transparency to know the salaries of every other colleague which would mean a breach of confidentiality for others.</p> <p>EXAMPLE: The employer is contacted by a private pension company to obtain accurate info about the employee in case the employee changed their first name or contact details, in order to be able to contact the employee and keep them informed about their pension. This could be a legitimate interest of the private pension company to obtain accurate data from the employer, which would also benefit the employee by allowing them to be contacted by the private pension company about their pension.</p>
--	---	---

4	24	<p><i>Historical or other kinds of scientific research.</i> Another important context where processing in the legitimate interests of third parties may be relevant is historical or other kinds of scientific research.³</p>	<p>OBSERVATION: It should be mentioned explicitly that the legitimate interest of a third party in processing personal data for scientific/historical research will not override the lawful basis of art. 9 for processing special data, as the case may be for conducting scientific research. For example: a doctor/clinic, even if it has the legitimate interest of conducting research in order to determine if the reference value of a certain marker has grown for the entire population/a fraction of it, that doesn't mean that other clinics and laboratories should or could send over special data among general data because of that legitimate interest.</p> <p>PROPOSAL: <i>Historical or other kinds of scientific research.</i> Another important context where processing in the legitimate interests of third parties may be relevant is historical or other kinds of scientific research, except if sensitive data are involved and the data subjects can be identified, then the processing of sensitive identifiable data (excluding statistical data) needs to comply with article 9 GDPR.3</p>
5	26	<p>In this context it should be recalled that, in case personal data will be processed for a purpose other than that for which the data were initially collected, the controller must check and ensure that the new purpose is compatible with the original purpose under Article 6(4) GDPR³⁹ (unless the data subject has given consent or the processing is based on EU or Member State law). Therefore, such compatibility assessment should, in general, be done in situations where personal data were initially collected in the legitimate interest of the controller and, then, are further processed in the legitimate interest of a third party.</p>	<p>OBSERVATION: Who has the responsibility of making sure that the new purpose is compatible with the original purpose? Does the original Controller have to act as a privacy consultant/lawyer and analyze if the interest of the third party is compatible with the original purpose based on which the Controller informed the data subject? What happens if the original Controller considers that the new purpose is not compatible with the original one, although the third party considers that it is compatible?</p>
6	27	<p>Nevertheless, it should be emphasised that Article 6(1)(f) GDPR may be invoked as a valid legal basis only if the necessity and balancing tests outlined below (see Section B and C below in this chapter) have also been carried out and the outcome of such tests was favourable to the controller.</p>	<p>OBSERVATION: It should be clearly stated that the third party is responsible for analyzing the necessity and conducting the balancing test.</p>
7	30	<p>It should be noted that, in practice, it is generally easier for a controller to demonstrate the necessity of the processing</p>	<p>OBSERVATION: The burden of demonstrating the necessity of the processing pursued in the interests of a third party should not be on the original Controller. The respective third</p>

		to pursue its own legitimate interests than to pursue the interests of a third party, and that the latter kind of processing is generally less expected by the data subjects.	party is acting as Controller regarding the information received and has all the obligations as mentioned in the GDPR. Para. 30 as it is makes the possibility of processing data based on the legitimate interest of a third party inapplicable, as no Controller will accept the responsibility of conducting a balancing test for another company with whom they have no relation whatsoever and thus not having access to all the information required to conduct such an analysis.
8	40	<p>The last paragrah that reads: „It is irrelevant whether or not the information revealed by the processing operation in question is correct and whether the controller is acting with the aim of obtaining information that falls within one of the special categories referred to in that provision.⁵⁰ Hence, according to the jurisprudence of the CJEU, the relevant question is whether it is objectively possible to infer sensitive information from the data processed, irrespective of any intention of actually doing so.”</p>	<p>OBSERVATION: The interpretation based on which, regardless if the information is correct or if the Controller was aiming at obtaining information that falls within the special categories of data, will have an unwanted impact in practice and is not within the spirit of GDPR. We will go back to asking for consent for each processing. The interpretation of what sensitive data is needs to be restricted to when Controller aims at processing such information. In such a case we will sign consent for processing inferred sensitive data when shopping for groceries online.</p> <p>EXAMPLE: If I go grocery shopping online and buy for my neighbor or for me chocolate that has artificial sweeteners instead of sugar, with this interpretation it means that the shop will process sensitive data which cannot be processed based on legitimate interest and will require my consent to store the info that I bought chocolate cake with artificial sweeteners, which mean I could have diabetes even if this info is not correct not the shop intended to process such information. Based on this interpretation, prior to processing that info I need to be prompted with a consent form for processing sensitive data - and if I don't consent, will I not be able to buy chocolate cake with artificial sweeteners? Another example of the catastrophic effect of such an interpretation: If I walk in a shop that has video surveillance and for some reason I have a limp, maybe I have a blister which makes me a bit uncomfortable when I walk so I limp, does it mean that the shop needs to prompt me with a consent form for processing sensitive data because you may assume that I have a medical condition based on which I limp? Or in case I'm in a wheelchair and on the CCTV footage which is stored for certain amounts of time you can see me in that wheelchair</p>

			and assume I have a medical condition that impedes me from walking? In all these cases based on the interpretation mentioned in para 40 the Controllers need to obtain consent.
9	52	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. ⁶⁰	<p>OBSERVATION: For a better applicability of para. 52 our opinion is that we need to differentiate between the commonly processed data in a given sector that are known by data subjects and the ones that are not known.</p> <p>EXAMPLE: CCTV in shops and different facilities is a common practice nowadays, therefore it is a reasonable expectation that when entering a store there will be a video surveillance system in place capturing images. And this situation is completely different from the processing of data by social media platforms, whereby although the processing is common for them it is not yet generally known by its users.</p>
10	53	Reasonable expectations do not necessarily depend on the information provided to data subjects. While the omission of information can contribute to the data subject being surprised of a certain processing, the mere fulfilment of the information obligations set out in Articles 12, 13 and 14 GDPR is not sufficient in itself to consider that the data subjects can reasonably expect a given processing. ⁶¹	<p>OBSERVATION: One of the reasons why the information obligation is set according art. 12-14 GDPR is in order to inform the data subjects about the processing the entity is conducting. We cannot assess the reasonable expectation of certain processing activities based on each individual. Maybe a 90-year-old person will not expect CCTV in a shop due to the technology the elder lived with, but a 20-something youngster will expect CCTV in a shop. What should the Controller do – switch the cameras on and off based on who enters the store? Stating that although you informed the data subject via an information notice is not enough, could lead to the inapplicability of art. 12-14 GDPR because the data subject will state that although they were informed via an information notice they did not read it and they did not expect certain processing and therefore the processing is not lawful. We need to take the rest of the actors into consideration, not only big tech firms with privacy notices made specifically to confuse you. We need to consider the rest of the entities as well, that could face a negative impact if whether they informed the data subjects or not it will be considered that the processing is not reasonable due to the fact that based on impossible to quantify criteria (reasonable expectation) the data subject did not expect a processing for which they were also informed. This could lead to asking for consent for every processing and making the legitimate interest lawful basis inapplicable</p>

			and we will be reducing the lawful basis of consent to check boxes no one reads and also the scope of consent will be washed away as people will give consent they cannot really withdraw.
11	72	After an objection, the controller shall no longer process the personal data unless there are overriding compelling legitimate grounds which take precedence over the interests and rights and freedoms of that person, which it is for the controller to demonstrate. ⁸² Thus, contrary to Directive 95/46/EC, the GDPR places the burden of proof on the controller, and provides a presumption in favor of the data subject. ⁸³	OBSERVATION: An example of how that compelling reason could look like would be useful in order to better determine how to handle a processing based on legitimate interest in relation to an opposition from the data subject.