Comments on the draft Guidelines 6/2020 of the European Data Protection Board

This paper only reflects the views of its author.

On 22 July 2020, the European Data Protection Board published its draft Guidelines 6/2020[1] *"on the interplay of the Second Payment Services Directive and the GDPR"* (hereinafter referred to as Draft Guidelines or Draft).

The Draft Guidelines, again, demonstrate the EDPB's legally erroneous interpretation of the contractual legal ground in the GDPR [Article 6(1)(b)], which results in inconsistent statements and unfulfillable requirements. On top of that, the EDPB is not able to get over its false, and never proved, idea that the contractual relationship is necessarily imbalanced to the disadvantage of the data subject.

1. Interpretation of Article 6(1)(b) of GDPR

Article 6(1)(b) reads that *"processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract".*

From the perspective of what "contract" means with regard to the parties in the context of the GDPR, one must read the following provisions as well:

- Article 22(2): *"a contract between the data subject and a data controller",*
- Article 49(1)(b): *"a contract between the data subject and the controller",*
- Article 49(1)(c): "*a contract concluded in the interest of the data subject between the controller and another natural or legal person".*

From these provisions, it should be clear that *"a contract to which the data subject is party*"—in Article 6(1)(b)—is not limited to the contract between the data subject and the data controller but the scope of this term is wider. It covers the following situations.

a) the data controller processes the data subject's data because the contract is only between them,
b) a data controller processes data related to two other entities (who are in a contractual relationship) from which at least one entity is a natural person. In this case, the requirement of Article 6(1)(b) is met, since the processing is necessary for the performance of ***a*** contract to which the data subject is party,
c) the data controller involves a third party (sub-contractor) to perform some actions in order to fulfil the contract between the data controller and the data subject. In this case, again, the requirement of Article 6(1)(b) is met, since the processing by both the data controller and the sub-contractor is necessary for the performance of ***a*** contract to which the data subject is party. This situation is also described in Article 49(1)(c)—a

[1] See at the following link
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202006_interplaypsd2andgdpr.pdf

contract concluded in the interest of the data subject between the controller and another natural or legal person—, which, if allowed as a derogation for specific situations, must be allowed in "normal" situation as well: Article 6(1)(b) incorporates this possibility as well.

The described interpretation is based on ***basic*** interpretation techniques (grammatical interpretation, systematic interpretation).

Based on the above, it is clear that the interpretation given by the EDPB is obviously legally erroneous in the following cases.

a) Subchapter 2.4 *[Lawful ground for granting access to the Account (ASPSPs)]*: ASPSPs have a contract with the data subject (payment service user) and the data subject has a contract with the PISP and/or AISP. Access to the payment service user's account by a PISP or an AISP is—therefore—*"necessary for the performance of a contract to which the data subject is party"*, namely the correct legal basis is, simply, Article 6(1)(b) and not the "legal obligation". In the context of a contract, "obligation" cannot be considered *per se* legal obligation, since, as also explained by many to the EDPB, with this logic, *any* obligation of the parties could be considered as legal obligation, and the entire contractual relationship would be based on "legal obligation": who could deny that payment for a service—as core obligation of one of the parties—is an obligation prescribed in civil law? However, this standpoint would contradict the EDPB's other erroneous standpoint, i.e. the data processing in case of non-performance of the contract is based on a legitimate interest. So, which one?
b) Chapter 4 *[THE PROCESSING OF SILENT PARTY DATA]*: as explained above, a silent party is a party to a contract with the client of a PISP/AISP/ASPSP, and his/her data must be processed by the PISP/AISP/ASPSP in order to perform the contract to which the silent party is a party. In this way, the requirement of Article 6(1)(b) is met. The silent party falls under Article 14. If the client and the silent party are both natural persons, the PISP/AISP/ASPSP is in relationship with two data subjects. If either the client or the silent party is not a natural person, Article 6(1)(b) still applies to the party who is natural person.

2. Scope of "contractual consent"

It was very encouraging to read that the EDPB acknowledged that there is contractual consent (Subchapter 3.2), because it shows that the EDPB realised that the contract means (mutual) consent between the parties, i.e. a contract cannot be concluded if the parties do not agree on the terms and the conclusion. In the light of this, it is, however, quite struggling how the EDPB is making attempts to limit the parties' autonomy to determine the content of their contractual relationship.

It is strange that, while the EDPB keeps insisting on the theory of "objective necessity", it writes about *"processing which is useful but not objectively necessary for performing the contractual service"* (paragraph 17). Like in the case of international agreements, in the case of any contract, nothing is agreed until everything is agreed. Therefore, it is impossible to

separate what is “useful” and what is “objectively necessary” regarding a contract because a contract is in this context a unit.

If something is “useful” in the context of a contractual relationship, it means that both parties agreed on the said conditions. Challenging this would mean that the EDPB knows better what a data subject wants? Can a data subject not agree to give access to whatever he/she wants which is not illegal (a PSD2 contract is *per se* not illegal)? Is it in harmony with the provisions of bank secrets and payment secrets (which are not mentioned at all in the Draft Guidelines, despite the fact that bank secret is one of the core elements of the relationship between a person and a financial institution)? And with the theory of information self-determination? I do not think so, the EDPB should accept that data subjects are not under “data protection guardianship”.

Paragraph 19 requires other legal basis for such “useful but not objectively necessary processing” but fails to determine: which one. Let us take the possibilities:

a) legal obligation, task carried out in the public interest or in the exercise of official authority task [points (c) and (e)]—obviously—are out of question since these cases represent external pressure, which is incompatible with the agreement of the parties,
b) vital interest [point (d)] is also out of question, since concluding such contract is not vital at all,
c) legitimate interest [point (f)] is similar to legal obligation, i.e. if legitimate interest is acceptable, it represents a pressure on the data subject (which, again, is in contradiction with the fact that the data subject agreed to the terms and conditions),
d) consent [point (a)] could be a possible legal ground but what is the difference between the contractual consent and consent? Nothing: nobody is forced to conclude contracts in question, and withdrawal of the consent means termination of the contract.

Simply put: in contractual relationships, regarding the elements of contractual nature of the relationship, unilateral legal grounds [such as consent in accordance with Article 6(1)(a) or legal obligation] cannot be applied due to the nature of the relationship of the parties.[2] The agreement of the parties (i.e. conclusion of the contract), however, represents the mutual “consent” of the parties.

The EDBP should reveal its legal analysis regarding the legal ground, since otherwise “revelations” are not convincing at all.

The EDPB’s erroneous idea of “objective necessity” (in addition to being impractical) might have serious negative consequences, namely it may destroy some objectives of the PSD2 directive, including to promote the development and use of innovative online and mobile payments. “Objectively necessary”—as translated into technology—means uniform technical solutions limited to the absolute minimum. This kills the innovation and competition on this

[2] It does not exclude that law regulates some aspects of the contractual relationship, but it does not change the contractual nature of the relationship and the legal ground. For example, data processing based on „necessary cookies” is based on contractual legal ground and not on „legitimate interest” (practically, it is absolutely senseless to create documents—balance tests—for what is allowed by law, while it absolutely fits into the logic of contractual relationship).

market, limits the data subjects' possibilities to choose the product suitable for their needs, since even "useful" solutions are out of the scope of solutions acceptable by EDPB. (It is worth mentioning that paragraph 79, by acknowledging the *"specifics of the service"*, further deepens the contradiction within the draft Guidelines.) This approach, in my view, violates even the GDPR, which clarifies in recital (4) that *"the processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."* The EDPB should clarify why "useful" data processing is out of the contractual legal ground.

3. Processing of special categories of personal data

This issue shows the serious faults of the GDPR.

a) Are provisions of Article 9 considered as legal grounds?

Since Article 9(2) – with one exception – does not mention the contract as legal ground, it is an important question whether a contract can be suitable legal ground for processing special categories of personal data. Although there are many examples of processing special categories of personal data in a relationship based on a contract [e.g. a vast variety of life, health, accident insurances, in addition to healthcare services – Article 9(2)(h)], this issue is not satisfactorily settled in the GDPR. Despite the fact that even the WP29 raised this problem[3] and concluded that—in the context of the GDPR—Articles 6 and 9 *"should be applied cumulatively"* (i.e. Article 6 is about legal grounds and Article 9 is about specific conditions), seemingly, the EDPB changed its approach and—both in Guidelines 05/2020 on consent under Regulation 2016/679 and in the Draft Guidelines—denies that performance of contract could be the legal basis of processing of special categories of personal data. But in this case, the EDPB should acknowledge that special categories of personal data *"which are manifestly made public by the data subject"* [Article 9(2)(e)] can be processed without any further condition, as well as, that only special categories of personal data can be processed for the purposes of *"the establishment, exercise or defence of legal claims"* [Article 9(2)(f)] while "normal" personal data cannot, etc.

b) Which point of Article 9(2) could be applied?

The Draft Guidelines state that only Article 9(2)(a) (consent) and Article 9(2)(g) (substantial public interest) can be applied for the cases falling under PSD2. The Draft Guidelines state that special categories of personal data—on the ground of "substantial public interest"—can be processed *"when all the conditions of Article 9(2) (g) of the GDPR are met"*, first and foremost, if there is any Member State law regulating a given case. This standpoint of EDPB is quite surprising, it demonstrates that the EDPB is not able to realise: rules designed to regulate the intervention of a state into the private life of people (i.e. where parties are—by constitutional law—in superior-subordinate relationship) cannot be used for the situation where a data subject voluntarily enters into relationship with a—legally—equal partner. To meet the EDPB's

[3] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217) - https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

guidelines, the Member States should allow the processing of *any* special category of personal data (since payments may be linked to any transaction of any type where processing of special categories of personal data may occur) and in *any* case (for the same reason as before). Such law would, surely, not meet any condition laid down in GDPR. (That is why the requirements laid down in paragraphs 52, 54 and 57 are not realistic: a service provider will very likely process special categories of personal data (more precisely personal data that may refer to special categories of personal data) but this depends on the client's habit (i.e. if the user has any transaction referring to special categories of personal data).

But in my view, Article 9(2)(g) is not applicable at all. The public interest behind the PSD2 is to increase pan-European competition and participation in the payments industry also from non-banks, and to provide for a level playing field by harmonising consumer protection and the rights and obligations for payment providers and users. But in the concrete case (i.e. when service providers may have access to the user's special categories of personal data) such access is based on the wish of the user who concluded a contract with the service provider. Therefore, the legal ground is the "consent" of the data subject (more precisely the "contractual consent" of the data subject): assuming an average user, it is very likely that the user is aware of his/her financial transactions, and it is the user who would like to have additional information or services by using the services of the service providers under such conditions that the two parties agreed on. The service provider does not know what kind of data it will have access to (and this circumstance is also irrelevant for it) or—if the service provider offers a service that focuses on special categories of personal data—the user has right not to conclude such a contract if he/she does not want.

In sum, the legal ground of the special categories of personal data is the "consent" of the data subject. This "consent" is demonstrated in concluding the contract with the service provider. The law may impose (mainly formal) requirements regarding giving this consent, but it remains "contractual consent", since in a contractual relationship a consent cannot be else but contractual consent. The EDPB should elaborate the interpretation of Article 9(2)(a) in this way.

c) What constitutes special categories of personal data?

The Draft Guidelines states that *"financial transactions can reveal sensitive information about individual data subject, including those related to special categories of personal data"* and *"even single transactions can contain special categories of personal data"* (paragraph 51). It must be noted, however, that "reveal" and "contain" are not the same, and, what is more important, transactions do not necessarily refer to special categories of personal data. A few examples: toothpaste can be bought both in a pharmacy and in a supermarket, or some medicines (e.g. some antifebriles) can be bought at petrol stations and in pharmacies as well, but these facts do not (or not necessarily) refer to or reveal any special categories of personal data; some may contribute to the campaign costs of different candidates, so from this it is hard to conclude their political belief; medicine can be bought for others (e.g. children, spouse, other relatives), etc., etc. The EDPB should be more cautious declaring some transactions as "revealing" or "containing" special categories of personal data. And it should not be forgotten that, assuming an average data subject, the data subject is aware of his/her

financial situation and expenditure (at least in broad outlines), *and* without the data subject's consent the service provider cannot have access to these data. So, the "harm" that the data subject may suffer is far from the significant.

* * *

The view that the controller is in a position of power and the data subject is vulnerable runs throughout the Draft Guidelines. This may be in line with the "classical" theory of data protection but is not in line with civil law relationships (among many others…). However, this generalising (and erroneous) approach culminates in such statements which, with minimal knowledge of the field, in this case payment services and the banking sector, are clearly unviable, impracticable and which practically could result in the impossibility of implementation of the rules in that field. The EDPB should review these draft Guidelines by considering the specificities of payment services and civil law in general. As a result, the definition of "consent" should be finetuned (especially in such situation that is covered by these Draft Guidelines) by respecting (and not restricting) the autonomy of the data subjects.

Zsolt Bártfai