DIGITALEUROPE

24 MAY 2019

Response to EDPB public consultation on draft Guidelines on performance of a contract for online services

Executive summary

DIGITALEUROPE welcomes the opportunity to provide its comments on the European Data Protection Board's (EDPB) draft Guidelines on the processing of personal data under Article 6(1)(b) of the GDPR in the context of online services.

We appreciate the EDPB's intention to ensure an appropriate use of the contract legal basis in the online context. At the same time, we find that the issues addressed are more generally applicable beyond online services. As such, we urge the EDPB to consider a broader scope in the final version.

In our response we'd like to point out areas where we find the draft Guidelines incorrectly apply the relevant GDPR provisions. As the trade association representing the technology industry in Europe, DIGITALEUROPE is in particular concerned with the impact that a restrictive interpretation may have on innovation in both technology and business models.

In particular, we highlight that:

- The relationship with the general principles applicable to processing justifies a more flexible use of contract as a legal basis and should be more accurately explained;
- Multiple legal bases, including contract, can apply to the same processing activities;
- Necessity needs to be interpreted in the broader context of a contract – including users' expectations in terms of personalisation and service improvement in today's online ecosystem – rather than merely restricted to what would otherwise be completely impossible without processing the data at hand;
- A restrictive interpretation of the contract legal basis should not be used to limit innovation or step into product design and development; and

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

- The final Guidelines should elaborate on the relationship between the contract legal basis and further processing as well as applicable ePrivacy rules.

Table of contents

General observations

Principles for processing and selecting the legal bases

Throughout the draft Guidelines there appears to be a conflation of the principles related to processing (Art. 5 of the GDPR) with the selection of the appropriate legal bases (Art. 6(1)). This is particularly evident with respect to the fairness and purpose limitation principles.[1]

For instance, the draft Guidelines state that '[c]ontrollers must take into account the impact on data subjects' rights when identifying the appropriate lawful basis so as to fully respect the principle of fairness.'[2]

We believe this conflation is misguided and leads the EDPB to an overly restrictive interpretation of the contract legal basis itself. Effectively, the EDPB seems to attach the relevance of the Art. 5 principles directly to the selection of appropriate legal bases, whereby the selection of an incorrect legal basis is automatically supposed to undermine the relevance of the principles.

However, the principles laid down in Art. 5 – which beyond lawfulness include fairness, transparency, data minimisation, storage limitation and integrity and confidentiality – remain fully applicable irrespective of the legal basis that is selected, subject to all relevant provisions in the GDPR.

The correct legal bases, by contrast, should be determined on account of what's appropriate in light of the specific purposes for processing. This is an objective determination from which the relevant application of data subject rights, which the GDPR as a whole is designed to protect, ensues.

'Generic' purposes

In the general observations, the draft Guidelines also stress that generic purposes stated in contract terms – in particular, improving user experience, IT security or marketing – as a rule contradict the purpose limitation and data minimisation principles and cannot be considered to be specific enough.[3]

---

[1] See, in particular, para 18. We note, in passing, that the draft Guidelines seem to unduly expand the reach of other GDPR provisions to the selection of an appropriate legal basis. For instance, para. 12 mentions an 'imbalance' between the controller and the data subject, suggesting that the selection of the legal basis should consider, if not remedy, such relationship. However, 'imbalance' is only mentioned in the GDPR (Recital 43) with respect to the consent legal basis.

[2] Para. 1.

[3] Para. 16. We note in passing that this interpretation seems to contradict the EDPB's own reading in para 45 that the purpose of 'service improvement,' which does not appear fundamentally different from 'future research,' may be able to rely on legitimate interest or consent.

We disagree with this position. There is nothing unclear about the use of data to improve products and services and there is no evidence that data subjects do not understand this use. Moreover, for reasons of business confidentiality, and because product and service innovation requires experimentation and development over time, it is difficult or even impossible to be fully precise about the exact service or product being researched or developed in advance.

The EDPB position would essentially prohibit normal, everyday use of data for straightforward purposes such as development of new features in software or language personalisation tools on websites. We urge the EDPB to reconsider these examples.

Processing may fall under different legal bases at the same time

The GDPR provides that processing is 'lawful only if and to the extent that *at least one*' legal basis applies.[4] As the same data can be processed for multiple purposes, processing activities can be lawful under one or more legal bases, provided that the relevant requirements are met.

Relying on more than one legal basis for the same processing activities does not contradict the controller's transparency obligations, so long as such legal bases are correctly identified.

Some examples of processing activities that may be covered by more legal bases are:

- The same personal data may be necessary in order to enforce a contractual duty, thereby falling under the contract legal basis, but also in order to comply with applicable legal requirements, thus being covered by the legal obligation basis.
- The same personal data may be processed to comply with relevant law (for instance, the NIS Directive),[5] thereby falling under the legal obligation basis, but also for the controller's own need to secure or prevent fraudulent use of its products, services or processes, which falls under the legitimate interest legal basis. The same data can indeed also be considered to fall within the contract legal basis to the extent that users will expect the service to provide a certain degree of security.[6]
- The same personal data may be technically necessary to deliver a service, thereby falling under the contract legal basis, but may also be processed for the controller's own R&D activities aimed at improving its products, services or processes, thus being covered under the legitimate interest legal basis.

[4] Art. 6, emphasis added.

[5] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[6] See Working Party 29 Opinion 2/2006 on privacy issues related to the provision of email screening services, p. 6.

As a consequence, we disagree with the EDPB's statement that 'it is generally unfair to swap to a new legal basis when the original basis ceases to exist.'[7] Processing may in fact still be lawful if one legal basis proves unavailable while others still stand.[8]

Understanding what is 'necessary'

The contract legal basis does not restrict data subjects' rights

The draft Guidelines refer to the European Data Protection Supervisor's (EDPS) necessity toolkit[9] and to CJEU case law[10] to advocate a narrow approach to defining necessity.

However, it should be noted that both the EDPS toolkit and the cases mentioned refer to the legality of Union or Member State law involving processing of personal data, not to contract performance. As such, they concern solely Art. 6(1)(c) or (e) rather than Art. 6(1)(b).

A restrictive construction is required when interpreting necessity as it relates to Union or Member State law given the restrictions that such law can impose on data subjects' rights, as evidenced by the GDPR's Art. 23.

However, the contract legal basis does not in itself restrict data subjects' fundamental rights, which remain protected by the GDPR framework in full. We find, therefore, that such a restrictive interpretation is neither correct nor warranted.

More generally, legal bases cannot be conceived as a way in which users' rights are limited. Quite on the contrary, Art. 6(1) requires a legal basis to be established so that such rights can be protected accordingly based on all relevant GDPR provisions.

Moreover, as highlighted in our general observations, the selection of a legal basis under Art. 6(1) does not undermine the applicability of the general principles for data processing laid out under Art. 5, which include purpose limitation and data minimisation.[11]

[7] Para 39.

[8] The GDPR itself contemplates that multiple grounds for processing can exist at the same time. Art. 17, for example, lists as a ground for erasure the withdrawal of consent 'where there is no other legal ground for the processing.'

[9] EDPS, 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit.'

[10] C-524/06 and combined cases C-92/09 and C-93/09.

[11] See also paras 14-15 of the draft Guidelines.

The context of a contract

Although we appreciate that contract law falls outside the scope of the draft Guidelines, we believe it is problematic to consider the contract legal basis without more specific consideration of contract law.

The draft Guidelines, in particular, appear to limit the use of the contract legal basis to situations where it would be altogether impossible to deliver a service absent the processing of the specific personal data at hand.

This reading, however, is not supported by the GDPR text, which refers to processing '*in the context* of a contract,'[12] thus suggesting a broader interpretation. This is in line with civil law, where contracts oblige contracting parties to comply with their provisions and the nature of the contract according to law, ordinary usage and good faith.

From this perspective, a contract's context must take into account all the relevant phases – the precontractual phase, the contract's execution, its performance, monitoring, enforcement and termination. So long as a given contract is legal, processing consistent with the purposes of such contract can legitimately fall within the contract legal basis.

In practice, there may be multiple reasons why processing may be necessary for the performance of a given contract, and each contract's specific context will need to be factored in to determine what falls into the contract legal basis. This might include activities such as enforcement of contractual rights clauses; compliance with contractual warranties; an international transfer in the context of a derogation; service personalisation; fraud prevention or security of processing.

'Less intrusive' processing

We are particularly concerned by the draft Guidelines' position that contractual necessity also entails an assessment as to whether the data processing at hand 'is less intrusive compared to other options for achieving the same goal.'[13]

In line with our observations above, we note that the quoted passage from the EDPS necessity toolkit is only relevant when assessing whether processing required by Union or Member State law is proportionate in the way it restricts data subjects' fundamental rights.

As already highlighted in our response, no such restriction occurs under the contract legal basis. We therefore find that extending considerations applicable in such specific and sensitive cases to contracts is neither correct nor warranted.

---

[12] Recital 44, emphasis added.

[13] Para. 25.

Necessary vs useful

Even with respect to the specific case law referred to in the draft Guidelines, we note that necessity should be construed more expansively.

The draft Guidelines contend that data that is 'useful but not objectively necessary' cannot fall into this legal basis. By contrast, the CJEU has held that processing that '*contributes* to the *more effective* application' of legislation – and, by extension, contracts – could be considered as necessary.[14]

At the risk of sounding overly simplistic, online messaging services were not strictly necessary when they were introduced if one wanted to write to family members or friends. But today it is difficult to argue that the associated processing of personal data is not necessary because SMS could achieve the same purpose in less intrusive ways.

Particularly in complex and diverse technological contexts, the 'combined, fact-based assessment' to determine whether 'less intrusive' data processing could achieve the same purpose would interfere with organisational, commercial and/or technical choices that should be left to service providers.[15]

To the extent that such choices are made in line with the relevant purposes for processing and the processing itself is objectively linked to such purposes, we see no reason not to allow reliance on the relevant legal bases (contract in this case).

Personalisation

The EDPB does acknowledge that personalisation can constitute an essential element of online services and can therefore be allowed under the contract legal basis.[16] However, in line with our observations above, we believe a more comprehensive interpretation of what should be considered as 'an integral part of using [a] service' in this context is necessary.

The draft Guidelines state that the contract legal basis cannot be relied upon if data is processed 'to increase user engagement,' that is, to improve the way consumers use a given service. However, many services are nowadays personalised by their very nature. Unlike a static web environment, today's average shopping service or music service can reasonably be expected to provide a personalised experience – for instance, a feature as simple as a message informing users about additional content included in their subscription based on content they've already interacted with.

---

[14] Para. 62, C-524/06, emphasis added.

[15] In case C-291/12 (see paras 51-52) the CJEU has considered the use of iris recognition as opposed to fingerprint recognition in passports, concluding that the former alternative is on the one hand not yet as advanced and on the other significantly more expensive, which justifies the use of the latter technology.

[16] Para. 54.

Requiring a separate legal basis as opposed to contract to cover the underlying data processing will run counter to users' expectations. This is particularly important in light of the EDPB's consideration of the mutual understanding between the controller and the data subject of what the contract's performance entails.[17]

Innovation and business models

Our point above illustrates our general concern that an overly strict interpretation of necessity, as that defended by the EDPB, creates negative consequences in terms of technological development and for companies' ability to place innovative business models on the market.

While we share the EDPB's intention of restricting inappropriate uses of the contract legal basis,[18] on a general level it is important to keep in mind that technological development is in essence the result of going *beyond* strict necessity and changing paradigms of product or service delivery.

A fair balance needs to be struck between the perceived impact on data subjects and companies' ability to innovate technology and services.

The freedom to conduct business, including contractual freedom, is an essential part of how our market-based economy operates. It should be up to companies to define the conditions under which they offer their services, the features they integrate, the features they make optional to their users as well as the most appropriate way to monetise a given service (including behavioural advertising).

So long as a company is compliant with the law, can be held accountable, follows a risk-based approach, provides transparency and control to its users and integrates privacy in its design process, it should be left to decide how it differentiates itself in a market and what products and features it offers to its users. Indeed, privacy settings and control tools are increasingly becoming market differentiators.

A restrictive interpretation of the contract legal basis should not be used to limit innovation or step into product design and development.

Missing parts

Contracts and further processing

The GDPR allows further processing for compatible purposes for all legal bases except consent and processing based on Union of Member State law.

[17] See in particular para. 32.

[18] Para. 5 of the draft Guidelines.

We encourage the EDPB to include in the final Guidelines an analysis of Art. 6(4) in relation to contracts. We believe such an analysis could help to arrive at a broader interpretation of the contract legal basis, in line with our points above.

Relationship with ePrivacy

Particularly because the draft Guidelines expressly focus on online services, we regret that they only vaguely refer to the need for controllers to comply, 'where applicable,' with ePrivacy legislation.

As a matter of fact, the ePrivacy Directive[19] – and even more so the proposed ePrivacy Regulation[20] – will as a rule always apply in the online context. A more detailed analysis of the application of the ePrivacy framework is therefore needed.

Such analysis is particularly important because the draft Guidelines' strict interpretation of contractual necessity is to an extent compensated by recognising that other legal bases – in particular legal obligation and legitimate interest – can be invoked. The ePrivacy framework, however, lacks these two legal bases.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Senior Policy Manager for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

[19] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

[20] COM(2017) 10 final.

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Airbus, Amazon, AMD, Apple, Arçelik, Bosch, Bose, Brother, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Facebook, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, MasterCard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: Nederland ICT, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK