Centre for Information Policy Leadership
Hunton Andrews Kurth

23 May 2019

Comments by the Centre for Information Policy Leadership on the European Data Protection Board's Draft Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects

Adopted on 9 April 2019

On 9 April 2019, the European Data Protection Board (EDPB) issued its Draft Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects (Draft Guidelines or Guidelines).[1] The EDPB invited public comments on this document by 24 May 2019.

The Centre for Information Policy Leadership (CIPL)[2] welcomes the opportunity to submit the comments and recommendations below as input for the EDPB's final Guidelines (Final Guidelines).

Comments

CIPL welcomes the EDPB's initiative to further explore contractual necessity as a lawful basis for processing as this has not previously been explored in detail by either the courts or regulators.

This topic raises some broad and complex questions and CIPL agrees with the EDPB that the full analysis of the concept of contractual necessity involves questions of contract, consumer and competition law that are outside the scope of the Guidelines. Therefore, the Final Guidelines should focus solely on the interpretation of data protection law. In this context, while paragraph 8 of the Draft Guidelines rightly states that they do not deal with issues around the validity of particular contracts,[3] paragraphs 9 and 13 condition the possibility of relying on Article 6(1)(b) on the prior fulfilment of obligations laid down in consumer protection and contract laws. While it is indisputable that a data controller is bound by all their legal obligations, CIPL suggests removing this statement to ensure consistency with the limited scope and remit of the Guidelines.

CIPL also welcomes the quality and considerations of the Draft Guidelines, and suggests generally for a more nuanced and subtle interpretation of Article 6(1)(b) as further explained below.

---

[1] Draft Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, available at https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-22019-processing-personal-data-under-article-61b_en.

[2] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth and is financially supported by the law firm and 75 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[3] *Supra* note 1 at paragraphs 8 and 9.

Additionally, CIPL welcomes the Draft Guidelines' recognition of the importance of choosing the right legal basis under Article 6(1) and the acknowledgment that Article 6(1)(b)[4] is intended to support the freedom to conduct a business, as guaranteed by Article 16 of the Charter of Fundamental Rights of the European Union.[5]

CIPL believes, however, that the criteria currently proposed in the Draft Guidelines for determining the applicability of the contractual necessity basis for processing, may in some instances, appear to be overly narrow and reach beyond the strict language of the GDPR. The current Draft Guidelines may have the unintended effect of preventing controllers from effectively applying Article 6(1)(b), even in appropriate circumstances where they have carefully assessed the necessity of the processing for the effective and comprehensive provision of their online services.

In particular, the Draft Guidelines do not sufficiently take into account the following points:

- **The reality that in today's digital world, personal data processing may form an essential part of the performance of a contract and this may vary greatly between different digital services, even when they appear to be similar on the surface**. The Draft Guidelines seem to assume that online services with similar prominent characteristics can have their core features and functionalities similarly and objectively classified between core and non-core. In the traditional offline or brick-and-mortar model, a clear distinction can be drawn between the contract and the associated personal data. In the digital economy, such distinction may be more difficult to draw along set lines[6] and requires a case-by-case assessment. This inextricable linkage of personal data and delivery of services has already been recognised on several occasions by the Article 29 Working Party, for example in its opinion in relation to smart metering[7] and on Data Protection Officers[8].

- **The need for the Final Guidelines remain flexible enough to allow for the future development of new technological, economic and contractual models involving the use of personal data**. The Final Guidelines should account for the complexity of modern data uses and the changing nature of digital services.

---

[4] "Article 6 GDPR - Lawfulness of processing. 1. Processing shall be lawful only if and to the extent that at least one of the following applies: […] (b) 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".

[5] "Article 16 of the Charter of Fundamental Rights of the European Union - Freedom to conduct a business. The freedom to conduct a business in accordance with Union law and national laws and practices is recognised".

[6] Electronic log data and metadata about an account or device may be generated as a result of user activity and may be required for the secure delivery of the service, for instance.

[7] Article 29 Working Party Opinion 04/2013 on the Smart Grid and the Internet of Things, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp205_en.pdf. The Working Party recognised the inextricable link between the performance of the contract to deliver the service and the data. It appears to have accepted that the personal data generated by the smart grid and, in the future, by the Internet of Things, is an essential part of the service supplied in a new environment.

[8] Article 29 Working Party Opinion 05/2017 on Data Protection Officers, available at https://ec.europa.eu/newsroom/document.cfm?doc_id=44100. The Working Party demonstrates that a hospital cannot provide healthcare safely and effectively without processing health data, such as patients' health records and that, consequently, the processing of personal data must be considered a core activity of the hospital, which necessitates the appointment of a DPO.

- **The need for the Final Guidelines to consider the notion of "compatible use, or not-incompatible use" as provided for by Article 6(4) of the GDPR and, more generally, to the risk-based approach** enshrined in the GDPR.[9]

- Throughout the Final Guidelines, **Article 6(1)(b) should be interpreted in light of Recital 44 of the GDPR that refers to processing "in the context of a contract"**. Such interpretation ensures Article 6(1)(b) remains applicable to modern data use contexts.

- **The assessment of what data processing is necessary for the provision of an online service should not be conducted in an *ex ante* manner, nor should it be conducted outside the context of the specific service offered.** It should account for all its offered functionalities and the specific business model involved.

- **From a policy perspective, the effect of the Guidelines and analysis of Article 6(1)(b) should not be considered in isolation but in relation to their impact and interplay with the choice of other legal bases in Article 6.** The overly narrow interpretation of the scope of contractual necessity as a legal basis for processing will impact the interpretation and adoption of other potentially relevant legal bases, such as legitimate interest or consent. Currently, given the high-bar for consent under the GDPR, it is reserved for limited contexts where individuals can make meaningful choices about the processing of their personal data and can effectively withdraw that consent without impact on the controller and the provision of services.[10] That may leave controllers compelled to seek legal basis in the legitimate interest ground for processing, which would be perfectly appropriate, but that must also be recognised by the EDPB and all DPAs. Therefore, the interpretation of Article 6(1)(b) should not be too narrow, if all the other grounds are also being narrowly interpreted in practice.

Part 1 – Introduction

1.1 Background

Paragraph 1

CIPL agrees with the EDPB that identifying the appropriate legal processing basis is of essential importance. The controller plays a central role in such identification as it defines the purpose and means of the processing. CIPL agrees that, in doing so, the controller must assess the impact of the data processing on data subjects, as this is part of the overall fairness and risk based approach of the GDPR. The Draft Guidelines provide however 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

[9] See CIPL paper on Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf.

[10] See Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Consent", 29 January 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_wp29_guidelines_on_consent-c.pdf.

fairness".[11] While CIPL agrees that the rights enjoyed by data subjects vary depending on the legal basis adopted by a controller, the Draft Guidelines appear to imply that controllers need to consider the rights available to data subjects before determining the legal basis (as opposed to ensuring that they respect the relevant rights once the legal basis is determined). CIPL believes that this interpretation needs to be nuanced, as a data controller should not base the selection of a particular lawful basis under Article 6 because it would afford or not afford specific rights to the data subject (see footnotes 2 and 3 of the Draft Guidelines). Rather, it should select a particular legal basis because it corresponds to the objective and essence of the processing.

In addition, the impact of a particular processing mandated by contractual necessity should be assessed in the broader context of the service that is being offered to individuals and that may not be delivered absent a particular processing. In other words, the assessment of the impact of the processing on data subjects should not go as far as necessitating changes to the service or some of its key features to reduce the potential impact on data subjects, where such processing is necessary to execute the contract. A fair balance needs to be struck between the impact of the data processing on data subjects and the controller's freedom to conduct business, which entails the right to structure it in a specific way and to select the appropriate lawful basis of processing within the applicable legal framework.

Furthermore, while CIPL agrees that fairness is a core and long-standing principle of data protection law, it does not believe that it should play a role at the time of selecting the appropriate legal basis for processing, which relies on an objective analysis. Compliance with the fairness principle should be verified during the risk assessment phase of the processing, when considering the impact of processing on rights and freedoms of individuals. During this phase, the controller analyses the level of risk of the processing with a view to identifying potential high risks to the rights and freedoms of individuals and applying the relevant safeguards and mitigating measures. In practice, of course, selecting the appropriate basis for processing and assessing the risks of the processing may be performed and documented simultaneously by the controller, often within a DPIA, too.

Finally, and more generally, a fair balance must be struck between the fundamental right of privacy protected by the Charter with the other rights of the Charter and the wider interest of society in enabling economic and social progress. As a reminder, Recital 4 of the GDPR very clearly states that "[t]he 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. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity". [12]

[11] *Supra* note 1 at paragraph 1.
[12] Recital 4 of the GDPR (emphasis added).

Summary of CIPL Recommendations:

- Clarify that the correct legal basis of the processing needs to be determined first, and that it is separate from assessment determination of fairness (evaluation of fairness normally being determined during the risk assessment phase).

- Weigh appropriately and reasonably the right to privacy with the wider interest of society in enabling economic and social progress and other fundamental rights protected by the Charter of Fundamental Rights of the European Union.

1.2 Scope of the guidelines

The Draft Guidelines "are concerned with the applicability of Article 6(1)(b) to processing of personal data in the context of online services" only.[13] CIPL believes that the scope of the Draft Guidelines is too narrow considering the diversity of organisations that rely on Article 6(1)(b). Companies in all industries and sectors, including online and offline services, need to rely on contractual necessity as a legal basis for processing. In addition, all companies as part of their digital transformation are increasingly relying on data processing and digital services to develop, sell and market their products and services. As a result, companies that used to have pure brick-and-mortar business models are now also providing online services in addition to their traditional services or products. Often, all of this is part of the same contractual arrangement. As a result, all organisations and all business models (and not just pure online service providers) would benefit from a better delineation and understanding of contractual necessity as a legal basis for processing personal data.

CIPL would also like express a broader concern with the suggestion, in paragraph 4 of the Draft Guidelines, that some business models are, by nature, less conducive to privacy protection. Indeed, CIPL would argue that online services, whether funded by user payments or ad-funded, should not, and do not, automatically make it "impossible in practice for the data subject to exercise any control over the use of their data". In fact, the spirit of the GDPR is precisely to ensure the accountability of organisations and effective transparency and user control, regardless of the industry and business model of the data controller. It is possible for any organisation to ensure the responsible use of data in compliance with the GDPR irrespective of its business model as the GDPR enables organisations to calibrate the accountability obligations to its risks.

Summary of CIPL Recommendations:

- Broaden the scope of the Final Guidelines to provide guidance for all organisations and business models rather than focusing on online service providers only.

[13] *Supra* note 1 at paragraph 7.

Part 2 – Introduction – Analysis of Article 6(1)(B)

2.1 General observations

Paragraph 12

When referring to the principle of fairness, the EDPB rightly mentions the "reasonable expectations of the data subject" and the need for the data controller to consider the possible adverse consequences on the data subject. The EDPB also mentions the need to consider the "potential effects of imbalance" between the data subjects and the controller.

CIPL believes that the reference to this type of imbalance is inappropriate in the field of data protection. The assessment of imbalance (and only when this imbalance is actually used to impose unfair provisions in the general terms and conditions) and the mission to protect the consumer in a commercial relationship clearly falls under the remit of consumer law, enforced by the relevant consumer law authorities. It is outside the scope of data protection and the GDPR[14] which aims to protect natural persons with regard to the processing of personal data.[15]

While both data protection law and consumer law may ultimately reach the same results (the imbalance between the controller and the individual in a commercial relationship may lead to unfair contractual terms and to the data processing going beyond the reasonable expectation of an individual), CIPL recommends that the notion of imbalance between the controller and the data subject be removed from the Final Guidelines for the following reasons:

- Such reference would contribute to creating the wrong presumption that an imbalance between the controller and the individual would necessarily lead to the processing being unfair under data protection law. As already mentioned, under the GDPR, the fairness test in Article 5 requires an analysis of the potential "surprising effect" of the processing[16] for the data subject only.

- Such reference ignores the reality of B2B relationships where a controller (provider) can process the personal data of an individual (customer) not acting as a consumer. In such cases, the notion of imbalance between the parties is irrelevant or may play in favour of the customer and not the provider.

Paragraph 16

In order to further analyse the notions of "purpose limitation" (Article 5(1)(b) of the GDPR) and "data minimisation" (Article 5(1)(c) of the GDPR), the EDPB refers to the 2013 Article 29 Working Party guidance on purpose limitation.[17] While CIPL highlights the high quality of these particular guidelines, this guidance is already six years old and is based on the Directive 95/46/EC. In light of the speed of

[14] The notion of "imbalance" is only mentioned in Recital (43) of the GDPR but only in relation to consent and in assessing whether it is freely given, in particular, where the controller is a public authority.
[15] See Article 1(1) of the GDPR.
[16] *Supra* note 1 at page 5, footnote 8.
[17] Article 29 Working Party Opinion 03/2013 on Purpose Limitation, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

innovation and numerous new data uses, CIPL recommends including more references and examples in the Final Guidelines that are relevant to the current state of technological developments and to modern data uses.

The guidance considers that the need for the purpose of the data collection to be "specifically identified" means it has to be "specific". However, Article 5(1)(b) of the GDPR requires the purposes to be "specified" under the purpose limitation principle, and there is no obligation for purposes to be "specific". While "specific" connotes exactness, things can be "specified" in general terms. This is indeed noted by the Article 29 Working Party guidance which subsequently states that:

> [t]he degree of detail in which a purpose should be specified depends on the particular context in which the data are collected and the personal data involved. In some clear cases, simple language will be sufficient to provide appropriate specification, while in other cases more detail may be required.[18]

Finally, if "specified" was to be understood as "specific", it is important to highlight that, in certain instances, the controller may not be able to be more specific as to the purposes of the processing than "improving users' experience" or "IT security purposes", for example. These purposes may actually be aligned with the individual's legitimate expectations that this processing is necessary for the performance of a contract or "in the context of a contract"[19] (see further analysis under paragraphs 45 and 46).

Summary of CIPL Recommendations:

- Remove the notion of "effects of imbalance" from the interpretation of fairness under Article 5(1)(a) in the Final Guidelines.

- Provide references and examples related to the current state of technological developments and modern uses of data in the Final Guidelines.

- Clarify that, depending on the context, the obligation to specify purposes of processing may not always mandate for specific details about the purpose of processing;

2.2 Interaction of Article 6(1)(b) with other lawful bases for processing

Paragraph 17

Contractual necessity is only one of six legal bases for processing personal data under the GDPR. CIPL agrees that care needs to be taken in identifying the correct legal basis at the outset of the processing. However, it is important to clarify that certain processing activities may be lawful under more than one legal basis. In the context of a contractual relationship, there may be multiple purposes for which

[18] *Id*. at page 15 (see section on "How precisely, and in how much detail, should the purpose be specified?").
[19] See Recital 44 of the GDPR "Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract" (emphasis added).

different processing operations are necessary. Likewise, a variety of purposes may exist and not all purposes may be fully known at the outset.

Article 6 of the GDPR confirms that "[p]rocessing shall be lawful only if and to the extent that at least one of the following [legal bases] applies". The language of "at least one" would tend to suggest that more than one legal basis may serve as lawful grounds for processing (assuming that the relevant requirements are met).

Summary of CIPL Recommendations:

- Clarify that within data processing, there may be more than one legal basis to legitimise various processing operation.

2.4 Necessity

Paragraph 23

CIPL agrees with the EDPB that following the *Huber* case,[20] "the concept of necessity has an independent meaning in European Union law, which must reflect the objectives of data protection law".

The EDPB goes on to note that "Article 6(1)(b) will not cover processing which is useful but not objectively necessary for performing the contractual service".[21] While CIPL agrees with this view, it is also important to ensure that the concept of "necessity" can be reasonably relied upon. Some sections of the Draft Guidelines appear to adopt a restrictive approach to the concept of necessity – one that effectively excludes all processing which is not absolutely and strictly required for the "main object" of the contract (a concept which itself is given a very narrow interpretation[22]). Indeed, the Draft Guidelines seem to suggest that contractual necessity is only available where the controller is "able to demonstrate how the main object of the specific contract with the data subject cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur".

This approach effectively amounts to a "but for" interpretation of "necessary" – i.e. processing is only necessary where it would effectively be impossible for the contract to be performed "but for" the processing activity taking place.

However, in *Huber*, the CJEU appears to have rejected such a strict "but for" interpretation of "necessary" which was offered by its own Advocate General.[23] In *Huber*, the court adopted a more flexible definition of "necessary" by holding that processing can be deemed "necessary" in circumstances where it allows the relevant objective at hand to be achieved more easily. The CJEU held that processing could be "necessary" if such processing "contains only the data which are necessary" for the relevant objective and allowed the relevant objective to be more effectively achieved:

[20] Case C-524/06, *Heinz Huber v Bundesrepublik Deutschland* (16 December 2008).
[21] *Supra* note 1 at paragraph 25.
[22] *Id.* at paragraph 30.
[23] See *Huber*, Opinion of Advocate General Poiares Maduro, at paragraph 29 (3 April 2008).

> The centralisation of those data could be necessary, within the meaning of Article 7(e) of the [Data Protection Directive], if it contributes to the more effective application of that legislation as regards the right of residence of Union citizens who wish to reside in a Member State of which they are not nationals.[24]

Huber demonstrates that the concept of necessity is largely fact-based and should be considered in light of the specific circumstances (i.e. the context) of the processing and the purpose it aims to achieve.

The decision in *Huber* has been applied to the "legitimate interests" test by the UK Supreme Court, in the case of *South Lanarkshire Council v. Scottish Information Commissioner*.[25] In this case, the UK Supreme Court considered the *Huber* decision and held that "it is well established in [EU] law, that at least in the context of justification rather than derogation, that "necessary" means "reasonably" rather than absolutely or strictly necessary".[26] The Court further confirmed, "something may be necessary if it makes furthering the purposes of a legitimate interest more effective".[27]

To conclude, in both *Huber* and *South Lanarkshire Council,* the definition of necessity was found to be broader than strict "but for" necessity. Instead, necessity supported processing that made the purposes "more effective" or where such processing "contributes to the more effective application" of the objective, so long as no more data than necessary was processed. The Final Guidelines should reflect this case law.

Also, the Draft Guidelines appear to suggest that contractual necessity operates as a derogation or limitation on the right to personal data, and so should be interpreted narrowly.[28] CIPL believes this interpretation should be nuanced.

Article 6(1) forms part of the right to data protection – it is not a limitation on the right. It operates as a framework and safeguard by explaining the circumstances in which personal data can be processed – "Processing shall be lawful only if and to the extent that at least one of the following applies…". This view is confirmed by Recital 44, which simply states, "[p]rocessing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract".

Contractual necessity can be contrasted with other scenarios where the right to data protection is being truly limited, either by legislation or by other policy considerations (for example, Article 23 of the GDPR which allows data protection rights to be "restricted" in certain cases where it is "necessary and proportionate" to do so, or Article 49 of the GDPR, which contains "derogations [from the restrictions on transfers] for specific situations"). In scenarios where the right to data protection is being abridged, case law confirms that the "necessity" test should be applied in a restrictive manner. However, in cases like the present, where a controller is establishing legal basis for processing for its legitimate business purposes and individuals are contracting to receive goods or services, the right to data protection is not being abridged. In such cases, *Huber* suggests that "necessity" should be given a wider interpretation.

[24] *Supra* note 20 at paragraph 62.
[25] *South Lanarkshire Council v. Scottish Information Commissioner* [2013] 1 WLR 2421.
[26] *Id*. at paragraph 27.
[27] *Id*. at paragraph 23.
[28] See, in particular, footnote 18 in the Guidelines.

Finally, this case law is also aligned with the text of the GDPR itself, which contemplates and enables data processing for "not-incompatible" purposes with the original purpose when the original processing is based on contractual necessity. This further endorses the view that the concept of "necessity" under the contractual necessity test of Article 6(1)(b) does not have to be interpreted narrowly (see further explanations in the next section below).

Paragraphs 24 - 25

Under Article 6(1)(b) of the GDPR, necessity also encompasses the concept of proportionality. CIPL believes this has not been sufficiently considered in the Draft Guidelines. Both case law and regulatory guidance reiterate that necessity and proportionality are closely related legal concepts that need to be considered together.[29] Processing activities can be considered proportionate if they result in a more effective application of the objective of the contract. The Court of Justice has considered the application of proportionality in Directive 95/46/EC.[30] One of the issues examined in *Michael Schwartz v Stadt Bochum* was whether the use of fingerprints rather than iris recognition was a reasonable choice for the public body. The Court accepted that the public body had made its choice taking into account a number of factors, including the cost of an iris recognition system and the stage of development of such systems. These are effectively commercial considerations that were deemed proportionate. The same reasoning will likely apply to the interpretation of Article 24 of the GDPR which provides that the controller shall implement appropriate technical and organisational measures to ensure that the processing is performed in compliance with the GDPR, taking into account, "the nature, scope, context and purpose of processing". The weighing of these factors and the necessity of the chosen measures will lead to an assessment of their proportionality (including on the commercial considerations).

Paragraph 25 of the Draft Guidelines states that the assessment of whether certain data processing is "necessary" for the purposes of Article 6(1)(b) "involves a combined, fact-based assessment of the processing 'for the objective pursued' […]". In paragraph 30, the Draft Guidelines refer to the "objective of the service", which seems limited to one "particular aim" or "purpose" of the service contracted. CIPL cautions against suggesting that an online service can have only one objective purpose, determined by the broad category of services it is believed to belong to. This is suggested again in paragraph 50, where the Draft Guidelines indicate that any purpose "separate from the objective purpose of the contract between the user and the service provider" is "not necessary for the performance of the contract at issue" and therefore falls outside the scope of Article 6(1)(b).

The standard proposed by the Draft Guidelines appears to exclude useful processing as not necessary, and seems to go beyond the intention of the GDPR. For example, Recital 44 suggests that useful processing should be included in the determination of what constitutes necessary processing under Article 6(1)(b). Delivering online services frequently involves processing data in ways that may not be immediately visible, but which is essential to the comprehensive provision of a quality service. This may include processing to make a service more accessible, faster, more reliable and secure and more attractive. Under the test proposed by the Draft Guidelines, these aspects appear only be considered as

[29] The European Data Protection Supervisor (EDPS) itself recognises the close relationship between necessity and proportionality. After adopting a toolkit on necessity, it considered that it needed to complement it with proportionality guidelines (Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, available at https://edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf).

[30] See Case C-291/12, *Michael Schwartz v Stadt Bochum* (17 October 2013).

"useful" and, therefore, would be excluded from the assessment of contractual necessity, even though they are absolutely central to the nature and the quality of the service being provided and in line with expectations of individuals.

Useful processing should, therefore, not be excluded from the understanding of what constitutes necessary processing. Instead, each online service should be considered in its entirety and with its specific characteristics. The assumption that users "request" only specific functionalities of a service that are more prominent or obvious than others does not reflect the way in which online consumers decide which service they use. Each user will be driven by different motivations when choosing one online service provider over another, including because one service provides specific functionalities that the other does not provide. In these cases, such features and the processing of personal data to enable them are part and parcel of the service being offered, and should be covered by Article 6(1)(b). This does not mean, of course, that all processing would be covered under Article 6(1)(b). Boundaries should be defined by the EDPB in a pragmatic and nuanced manner in line with these considerations.

The EDPB also mentions the need to perform a "realistic, less intrusive alternatives" test to ascertain whether the processing is necessary for the performance of a contract. However, such a test should not go as far as impacting too substantively on the freedom to conduct a business, such as by necessitating a change in the controller's business model and freedom to propose a particular product or service with specific features or characteristics. As a result, when assessing what is a "realistic" alternative, the controller's existing business model and service characteristics as well as the cost of alternatives should be taken into account in line with the interpretation of the concepts of necessity and proportionality described above.

Lastly, CIPL believes that the Draft Guidelines missed the opportunity to refer to Article 6(4) of the GDPR in enabling the personal data originally processed on the basis of contractual necessity to be further processed for purposes compatible (or "not-incompatible") with the original purpose. The text of the GDPR clearly permits reliance on Article 6(4) for all legal bases except for consent and processing based on Union of Member State law.[31] This also provides further evidence of an intended broader interpretation of "contractual necessity" than that put forward in the Draft Guidelines.

[31] See Article 6(4) and Recital 50 of the GDPR which explains that "[i]n such a case, no legal basis separate from that which allowed the collection of the personal data is required".

Summary of CIPL Recommendations:

- Apply the CJEU test defining "necessity" in line with the text of the GDPR, judicial precedent and the guidelines of the EDPS.

- Recognise that a service may have more than one purpose.

- Acknowledge that useful data processing may be included in the interpretation of Article 6(1)(b).

- Reframe the analysis of necessity on the basis that contractual necessity is not a derogation or limitation on the right to protection of personal data.

- Recognise that potential costs of implementation may be a relevant factor in assessing less intrusive means under the necessity test.

- Clarify that the contractual necessity legal basis also enables data processing for compatible, or not-incompatible, purposes under Article 6(4) GDPR.

2.5 Necessary for the performance of a contract with the data subject

Paragraph 26

CIPL suggests the EDPB to consider in the Final Guidelines that generally, the performance of a contract is not instantaneous, but rather the contractual relationship between the parties may vary during its lifetime and this depends on the type of products or services at stake and the different options selected by the customer. What is "objectively necessary for performing the contractual service" may go beyond an analysis at the particular individual level or a specific transaction at a given time. It should be balanced against the more general benefits for both the individuals and the controller. Such is the case, for instance, where processing of data is required to improve the products, perform some assessment of product returns, deploy a product recall, analyse and fix potential technical flaws or receive feedback on user experience. In such cases, it is clear that the processing of data is necessary in the context of the contractual relationship.[32]

Paragraphs 27 - 28

The EDPB refers to the Article 29 Working Party opinion on the notion of legitimate interests of the data controller[33] to point to the difference between processing that is genuinely necessary for the performance of a contract and terms that are "unilaterally imposed on the data subject by the controller".

CIPL believes that such difference is not always relevant, in particular, when processing is performed for security or for fraud prevention purposes. In these specific cases, terms are "unilaterally imposed on the data subject by the controller" while at the same time necessary for the performance of the contract.

[32] See Recital 44 of the GDPR.

[33] Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

Paragraphs 31-34

With respect to contracts for digital services, the EDPB notes that a contract cannot artificially expand the categories of personal data or types of processing operations that the controller needs to carry out for the performance of the contract within the meaning of Article 6(1)(b). CIPL agrees that a contract for digital services cannot superfluously require the collection and use of data in an unlimited manner. However, the Final Guidelines should also make clear that what is "necessary" cannot just be an assessment of whether a service can technically be offered in a way that is stripped of certain features that would prevent the need to engage in certain processing. Such clarification will avoid limiting Article 6(1)(b) to a product or service's most basic functions to the exclusion of additional features.

In fact, what is necessary for company A to provide a service may differ from what company B would need to provide a service that, on the surface, has the same basic functions. Online services are provided "as-is" and the interpretation of Article 6(1)(b) should not prevent this, providing they comply with the GDPR in all aspects.

The Final Guidelines should further make clear that controllers can rely on Article 6(1)(b) as the legal basis for processing not just for the initial version of an online service, but also for its subsequent versions and updates. Indeed, controllers may update their online services over time, for instance, by adding new features or updating existing ones. Where relevant, controllers should be able to rely on Article 6(1)(b) as the legal basis for such new or updated processing, providing, of course, that all the criteria in Article 6(1)(b) are still fulfilled. In other words, the moment a given data processing starts (whether as part of the initial launch of the overall online service or later as part of an update thereof) should have no bearing on the legal basis that can be used. Otherwise, this would create an artificial imbalance between existing companies who cannot rely on Article 6(1)(b) as the legal basis for new or updated features they launch and new entrants who will be able to, although they will process personal data in exactly the same way and for exactly the same purposes.

The EDPB refers to the notion of "mutually understood contractual purpose" on which the controller and the individual must agree. In doing so, the controller should rely on the "reasonable data subject's perspective" to justify the necessity of its processing.

CIPL recommends that the EDPB take into account the fact that, generally, the notion of "reasonable data subject" and "average data subject" in the provision of online services is constantly evolving and should be assessed in this specific context (and not just from the traditional perspective of a "brick-and-mortar individual").

As a result, Example 1, under paragraph 34 of the Draft Guidelines, should be amended to include that when products are shipped to a pick-up point, it may still be necessary for the performance of the contract to process the individual's home address. For instance, if the shipped product needs to be replaced or repaired, the data subject would expect that the controller knows the address of its client, to be able to contact him/her to ship an additional product or to identify another pick-up point. Moreover, the controller may need the address to identify the individual, and to authenticate an order, or the use of credit card and to prevent fraudulent orders (e.g. a billing address is required for the credit card associated with the order).

Paragraph 36

The EDPB provides that bundling of services that can be reasonably performed independently of one another may not rely on Article 6(1)(b) as a lawful basis for processing. Again, as part of the freedom to conduct a business and the freedom to contract, CIPL believes that as long as appropriate transparency is provided to the data subject, the parties should be able to agree on a "contractual object" that includes the bundling of services (provided that it otherwise complies with contract and consumer law, of course). In other words, the bundling of services should not render the processing unfair *per se* if such processing is transparent to and aligned with the reasonable expectations of the individual.

In addition, the Draft Guidelines seem to suggest that each service has a single "main object" that is objectively necessary to perform the contract, while all other features and functionalities are ancillary to that main object and therefore not requested by the user. As a result, such "ancillary" aspects of the service may not rely on Article 6(1)(b). This assumption, in the Draft Guidelines, may not reflect the reality of how consumers decide which services to use. Users may choose one service over another precisely because the service provider offers a wider array of functionalities than its competitors do. Some of these functionalities may be classified as non-essential or not the "main object" of the contract (and may not be used by some customers). Yet, the offering of such features and processing of personal data to enable them are in fact part and parcel of the whole service chosen by the consumer and, therefore, controllers should be able rely on Article 6(1)(b) for such processing.

Furthermore, as part of the definition of what is necessary for the "performance" of a contract, the Final Guidelines should reflect the GDPR's approach. As further explained below, the approach should include an evaluation of various factors, including the controller's and individual's perspectives.

The concept of "performance" should be interpreted consistently across EU Member States, according to applicable contract law that the GDPR is unable to modify. For example, under Irish contract law, "performance" refers to the fulfilment by a party to the contract of his or her contractual obligations under the terms of the contract. Similarly, the UK ICO recognises in its Guide to the GDPR that performance under contractual necessity includes processing "to fulfil your contractual obligations".[34] Therefore, in these two examples, the concept of performance enables considerable flexibility in the sense that, depending on the circumstances and the terms of the contract, effective performance may take the form of entire performance or something less than that (i.e. substantial performance). Finally, civil law countries also share the view that performance is a flexible concept. There, the contract obliges the contracting party to comply with its provisions and the nature of the contract according to law and ordinary usage and with reference to good faith. What emerges from this analysis is that "performance" may be wider than what the Draft Guidelines currently seem to suggest.

As mentioned earlier in this paper, Recital 44 of the GDPR also supports the view that "performance" should be interpreted consistently with the above (i.e. in a broader and more flexible manner). It states that "[p]rocessing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract". Recital 44 covers the two elements of Article 6(1)(b) – processing for the performance of a contract or in order to take steps prior entering into a contract - and, importantly,

[34] See the ICO Guide to the GDPR which states that "you can rely on the contractual necessity basis if you need to process someone's personal data: to fulfil your contractual obligations to them" (emphasis added), available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/.

does not mention the term "performance" but rather refers to "the context" of a contract. A literal reading of Recital 44 suggests that "the context" of a contract refers to the circumstances in which a contract is entered into and performed. Context is best understood as encompassing the "performance" of the contract without being exactly synonymous with it.[35] Context would thus include the EDPB's consideration of both the controller and a "reasonable data subject's perspective when entering into the contract" (see paragraph 32 of the Guidelines).

CIPL agrees with the EDPB that numerous factors should be considered when assessing the necessity of processing activities in the "context" of a contract, including the "exact rationale of the contract" and its "substance and fundamental objectives" (see paragraph 33 of the Draft Guidelines).

The Article 29 Working Party also recognised the role that an individual's expectations play in this assessment:

> "by setting up filtering systems, email providers can also be considered as ensuring the performance of the service contract with their customers, who expect to receive and send emails with a certain degree of security. Accordingly, the processing of data in which email service providers are engaged when they set up filtering systems may also be legitimised under Article 7 b of the Data Protection Directive which foresees the processing of data "necessary for the performance of a contract to which the data subject is a party".[36]

The Article 29 Working Party clarified here that individual's expectations can include providing the service with a "certain degree of security". It goes without saying that controllers and individuals commonly expect services to be reasonably secure and protected against fraud. This is already recognised in several EU legal frameworks, such as, for instance, in Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights,[37] the E-commerce Europe Trustmark Code of Conduct,[38] as well as the Payment Services Directive (PSD2) EU 2015/2366[39] and Regulatory Technical Standards on strong customer authentication and secure communication under PSD2[40] (the objective of which is to reduce fraud and enhance the level of safety and security in

[35] The reference in Recital 44 to "intention" ties in with the reference in Article 6(1)(b) to taking steps prior to entering into a contract.

[36] Article 29 Working Party Opinion 2/2006 on privacy issues related to the provision of email screening services, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp118_en.pdf at pages 6 and 7.

[37] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, available at, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32011L0083&from=EN#ntr5-L_2011304EN.01006401-E0005.

[38] E-commerce Europe Trustmark Code of Conduct, available at https://www.ecommercetrustmark.eu/the-code-of-conduct/.

[39] Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, available at https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en.

[40] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0389.

online payments). Consequently, processing activities required to reasonably provide a "certain degree of security" can fall within "processing necessary for performance of a contract with the data subject" or be recognised as a compatible purpose under Article 6(4).

As the EDPB notes, "the mutual perspectives and expectations of the parties to the contract"[41] must also be considered. One cannot solely assess the contract via the prism of the expectations and benefits to the individual. The benefits to and requirements of the controller, as well as the individual, need to be considered in determining what is necessary in the context of a contract. In an online agreement, an individual may freely agree, as part of the contract, to the processing of their data in specific ways or for specific purposes. Performance of the contract is achieved when the services are provided and the individual delivers the personal data for the agreed purposes. In other words, both parties have to perform their part of the bargain. The processing by the controller is necessary for the performance by both parties.

In summary, the text of Article 6(1)(b) of the GDPR and the supporting Recitals, the data processing principles and the CJEU's definition of necessity all support a more nuanced and flexible approach than that which seems to be suggested by the Draft Guidelines.

Summary of CIPL Recommendations:

- Revise the narrow approach to "necessity" in the Draft Guidelines in line with the text of the GDPR and its supporting Recitals, data processing principles and the CJEU's definition of necessity.

- Recognise the importance of freedom to contract.

- Recognise the evolving notion of a "reasonable data subject" in the context of digital services.

- Make clear that multiple processing activities may be necessary in the context of or performance of a contract.

2.6 Termination of contract

Paragraphs 38-42

In the context of contract termination, the EDPB considers that when the contract ends, the processing of data will no longer be necessary for the performance of that contract and as a result, the controller must stop the processing. In addition, it considers that it is unfair to rely on another legal basis than the one originally selected at this occasion.[42]

CIPL believes, however, that the EDPB should account for situations where processing has multiple legal bases. For example, processing might be lawful under both contractual necessity and necessity to comply with a legal obligation. Where legal obligations may not be precise enough or may differ from one country to another and the data controller wishes to apply a uniform standard for all its customer relationships, relying on contractual necessity may be more relevant and consistent than relying on

[41] *Supra* note 1 at paragraph 33.
[42] *Supra* note 1 at paragraphs 38 and 39.

different legal bases depending on the different countries involved. Should the contract end, processing under contractual necessity may not continue, but processing for purposes of complying with a legal obligation may still be lawful in certain jurisdictions. This would not be a "swapping" of legal bases but merely a continuation of the lawful processing under the legal obligation basis under Article 6(1)(c). For example, when the contract terminates, data must be kept to be able to evidence the organisation's compliance with applicable tax and accounting laws.

Moreover, the EDPB considers that if controllers keep records for legal purposes, including the establishment, exercise or defence of legal claims, they need to identify a legal basis at the outset of the processing and they need to communicate clearly from the start how long they plan to keep the data after the termination of the contract.

CIPL believes that, as a general rule, processing to monitor and enforce contractual terms (either to reach termination or otherwise), and until a relevant statute of limitation expires, should not be understood to be separate from the performance of the contract, but can be carried out on the basis of Article 6(1)(b). Also, it is customary for contracts to provide that, in the event of termination, certain accrued rights and obligations will remain binding on the parties (for instance, obligations around maintaining confidentiality, non-compete clauses or intellectual property rights). This means that the contractual necessity legal basis may continue to operate in certain post-termination scenarios.

Finally, legal claims and disputes may not always occur after the contract is terminated but during the contract's execution itself. Any legal claims or disputes that occur during the contract's execution or after full implementation, such as challenging some contractual elements or simply requesting full contact execution (for instance, payment or execution of a warranty) keeps the contract alive and the processing of personal data necessary to it. The Final Guidelines should account for this point.

Summary of CIPL Recommendations:

- Confirm that processing may have multiple legal bases.

- Acknowledge that processing to monitor and enforce contractual terms is part of the performance of the contract and such processing can be based on Article 6(1)(b).

- Recognise that Article 6(1)(b) can serve as a lawful basis for processing in the case of legal claims and disputes.

Part 3 – Applicability of Article 6(1)(b) in Specific Situations

In this specific section of the Draft Guidelines, the EDPB discusses some processing activities that commonly rely on the contractual necessity legal basis and finds that some of these may not meet the requirements of Article 6(1)(b). However, this should be aligned with the EDPB's suggestion, in sections 2.4 and 2.5 of the Draft Guidelines, that a nuanced assessment of the contract – its necessity, determination of contractual purpose, and understanding the data subject and controller's mutual perspectives and expectations – is required.[43] Otherwise, this may lead to creating a general presumption that certain processing activities, considered in the abstract, are not supported by

[43] *Supra* note 1 at paragraphs 25, 30 and 32 in particular.

contractual necessity, where in fact such assessment should be done *in concreto* by the controller in line with legal requirements and case law of the CJEU.

Additionally, the EDPB should not make determinations on whether certain types of processing activities are "fit" for processing under the contractual necessity basis, where such determinations contradict the text of the GDPR. For example, the EDPB considers that processing for fraud prevention involving monitoring and profiling customers may not be objectively necessary for contract performance. Yet, Article 22(2)(a) of the GDPR recognises expressly that decisions solely based on automated processing, including profiling, may be necessary for entering into or performing a contract. This supports CIPL's view that profiling (whether or not involving decisions based solely on automated processing) can be justified under the contractual necessity legal basis depending on the particular circumstances at stake.

Summary of CIPL Recommendations:

- Reconsider including pre-determinations of types of activities that may not rely on Article 6(1)(b) of the GDPR to avoid creating a presumption of inapplicability of contractual necessity to such activities absent an *in concerto* analysis.

3.1 Processing for "service improvement"

Paragraphs 45 - 46

The EDPB considers that contractual necessity is not an appropriate legal basis for processing for purposes of improving a service or developing new functions within an existing service. This includes the collection of organisational metrics relating to a service or details of user engagement.[44]

CIPL believes that this position is too "black and white" and does not reflect the reality of data processing. There are a number of reasons why continual service improvements may be objectively necessary for the performance of a contract or at minimum be considered as a compatible purpose:

- Any party to a contract has a legitimate expectation that the organisation offering a product or service will work to improve these over time, in particular in the context of online services which are changing on an ongoing basis. The EDPB asserts that "[i]n most cases, a user enters into a contract to avail of an existing service".[45] However, when it comes to online services, users rightly expect, and demand, that the service they receive improves over time, as technology advances, to benefit, for instance, from better connectivity, personalised experiences, performance, usability or security. Such improvements are part of the service they are seeking, and not something that is foisted upon them by the service provider. For example, a user who entered into a contract for an online email service in 2001 would not accept the provision of the version from 2001 in 2019. Indeed, they would likely reject such a service as not fit for purpose (given how functionality has evolved). Similarly, when purchasing smart home assistants, individuals are not only buying a product but also a service that they expect to continuously improve over time to provide a personalized experience. A user would likely not sign up to a static service that does not constantly learn and train itself in real-time and against real-life

[44] *Supra* note 1 at paragraph 45.
[45] *Id*. at paragraph 46.

usage. In other words, service improvement may be part of the contractual object on which the parties agree. In the modern digital age, this is just the way in which digital services are provided - with constant reiterations and multiple improved versions of the underlying technology.

- In addition, certain service improvements are inherently necessary to keep services reasonably safe and secure. Attackers are continually seeking vulnerabilities in systems, so those systems need to be updated from time to time (e.g. via security patches) to ensure that users get the service they contracted for in a reasonably safe and secure fashion.

- Further, many businesses will process personal data through customer satisfaction surveys and for business analytics to ensure that customers are getting the service for which they contracted and expect.

Finally, the compatible purpose interpretation under Article 6(4) also enables such further processing of service improvement metrics.

Summary of CIPL Recommendations:

- Reconsider the current view, in the Draft Guidelines, towards processing of personal data for service improvement under contractual necessity and further recognise the possibility of such processing under Article 6(4) of the GDPR on compatible processing, in the appropriate circumstances.

3.2 Processing for 'fraud prevention'

Paragraph 47

CIPL has similar concerns over the EDPB's view that processing for fraud prevention involving monitoring and profiling customers "is likely to go beyond what is objectively necessary for the performance of a contract with a data subject" and that another legal basis should be used. Determining the measures necessary to adequately protect the processing should always result from a case-by-case analysis rather than a broad presumption. Here, the Draft Guidelines appear to make an assumption for a very broad category of processing purposes, with no prior assessment of the specific contract or consideration of whether the fraud prevention processing in question necessarily entails "monitoring and profiling customers". As previously mentioned, CIPL believes that the appropriate use of contractual necessity cannot be determined via blanket assessments of hypothetical provisions but rather should consider the specific processing activities in light of the purposes of the specific contract and how such processing might increase the effectiveness of the contract and the quality of the service.

More generally, the provisions of the contract – construed under applicable law and, where applicable, ordinary usage and bona fide performance – might also require a reliable service for the two contractual parties (the user and the controller) to be reasonably protected against fraud and other security risks. Delivering reasonably safe online services could form an integral part of the contractual object or rights and obligations of many (online) service providers. This is clearly recognised in Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, in which protection against the fraudulent use of payment cards is considered an

essential aspect in distance contracts.[46] This is also in line with the E-commerce Europe Trustmark Code of Conduct in the context of which companies have made a commitment to offer safe payment methods and a safe web experience that meets consumer expectations.[47]

Furthermore, the rise in cybercrime, online fraud and identity theft over the last number of years has contributed to the emergence of new business models in which fraud prevention constitutes the primary object of a service offered to individuals. Such business models may include online identity theft monitoring, raising alerts when identity theft and/or financial fraud has occurred on the web or managing recurrent payments when a credit card is lost or stolen. Because these services are offered either as monthly/yearly subscriptions or as "one-offs", they constitute an absolutely necessary object of a contract between the controller and the individual.

In light of the above, CIPL recommends clarifying that Article 6(1)(b) can serve as a legal ground for processing personal data for fraud prevention, identity protection and cybersecurity purposes.

In addition, the fraud prevention cases listed at the end of paragraph 47 that would fall under Article 6(1)(b) appear to be too limited for two reasons:

- Fraud prevention may involve monitoring activities, for instance, where a company monitors the content of users' bios on its online service to verify that they do not show signs of impersonation or other fraudulent content; and

- Fraud prevention may require matching potential users with existing databases of fraudulent actors (maintained by either the data controller itself or a third party) or moderating the online service.

CIPL therefore recommends (i) not referring to processing for fraud prevention purposes that involves monitoring as being unable to rely on Article 6(1)(b) and (ii) clarifying that the fraud preventions cases outlined in the Draft Guidelines are to be considered as examples only and not as an exhaustive list of what is permitted or not.

Finally, it is important to note that Article 6(1)(b) is a valid lawful ground for processing in the following cases:

- Sending an OTP (One Time Password) to a phone as part of registering for, logging onto or authenticating in a secure service.

- Asking for 3 digits of a password or a PIN number to enable access.

- Where a user has enabled "one touch" fingerprint access, processing to make that work so the user can access the phone/apps or perform actions in those apps in which he/she has enabled to be responsive to "one touch" (e.g. a payment).

[46] *Supra* note 37.
[47] *Supra* note 38.

- ID and other document checks when the document is uploaded to make sure the document is not fake.

- Checks to make sure a person is a real human, not holding up a photo, wearing a mask or presenting a video of someone else (for instance, in the context of registering, logging in or otherwise requesting an action where if completed by an imposter it would have a negative or serious impact on the actual individual).

- Cybersecurity, fraud and identity theft monitoring and protection services.

Summary of CIPL Recommendations:

- Reconsider the current view, in the Guidelines, towards processing of personal data for fraud prevention involving monitoring and profiling customers under contractual necessity.

- Recognise that cybersecurity, online safety and protection have become key consumer expectations and are reflected by industry commitments regarding e-commerce.

3.3 Processing for online behavioural advertising

The EDPB sets out that, as a general rule, behavioural advertising does not constitute a necessary element of online services, and that organisations cannot rely on contractual necessity for the display of behavioural ads simply because these ads "indirectly" fund the services being provided.

It is important to highlight that the GDPR is agnostic in terms of the business models it regulates and their associated processing activities. Online advertising is a major business in the EU and is as lawful as offline advertising is.

While CIPL agrees with certain aspects of the EDPB's analysis, CIPL wishes to underline that there is significant difference of opinions and lack of clarity in the marketplace and among privacy professionals, lawyers and in the legal doctrine as to whether processing of personal data on the basis of Article 6(1)(b) would extend to funding the service through behavioural advertising.

CIPL cautions again against blanket determinations that specific processing activities linked to behavioural advertising are *de facto* permitted or prohibited as per Article 6(1)(b) outside of any case-by-case and facts-based analysis. CIPL also recommends including the notions of "reasonable user expectation", "freedom to enter into a contract" and the "objective purpose of the contract" agreed between the parties into its analysis (see previous paragraphs).

CIPL recommends the EDPB consider three different situations:

- Where the provision of online behavioural advertising is inextricably linked to the service provided (and the Draft Guidelines recognise that advertising can be part of the service[48]).

[48] See previous comments on page 2 above and paragraph 33 (last bullet point) of the Draft Guidelines.

- Where the provision of online behavioural advertising is legitimised under the "compatible, or not-incompatible use" purpose.

- Where the provision of online behavioural advertising is too remote from the contract core performance and the processing needs to rely on another legal basis.

Summary of CIPL Recommendations:

- Consider a more nuanced approach than the position that behavioural advertising cannot be deemed necessary for the performance of a contract.

- Conduct FabLab or smaller roundtables with the relevant stakeholders to "workshop" the different scenarios.

3.4 Processing for personalisation of content

CIPL agrees with the EDPB that personalisation of content can constitute an essential or expected element of certain online services. In this case, CIPL suggests that, in view of the low risk of the processing and the increasing expectation of personalised services by users, personalisation be considered as a legitimate expectation of a reasonable individual in the online environment.

CIPL further suggests amending Example 8 in the Draft Guidelines which currently notes that processing data to provide personalised product suggestions in an online marketplace cannot rely on Article 6(1)(b). For some online marketplaces the selection of products is vast and potential buyers who have no precise idea of the exact product they want to buy would likely expect to receive personalised product recommendations to assist them in navigating the marketplace and identifying the right product/service – as this is would be the case in any brick and mortar shop. In this case, processing would be necessary "in the context of a contract" or the "intention to enter into a contract".[49]

Summary of CIPL Recommendations:

- Consider processing for personalisation of content as a legitimate expectation of a reasonable individual and that processing to meet such expectations can be based on contractual necessity.

- Amend Example 8 to reflect that for some online marketplaces, personalised product recommendations may constitute an expected element of the online service and can be based on contractual necessity.

Conclusion

CIPL is grateful for the opportunity to comment on the European Data Protection Board's Guidelines on Contractual Necessity in the Context of the Provision of Online Services to Data Subjects. If you would

[49] See Recital 44 of the GDPR.

like to discuss any of these comments or require additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com, Markus Heyder, mheyder@huntonAK.com, Nathalie Laneret, nlaneret@huntonAK.com or Sam Grogan, sgrogan@huntonAK.com.