29 January 2018

**Comments by the Centre for Information Policy Leadership**

**on the Article 29 Data Protection Working Party's**

**"Guidelines on Consent"**

**adopted on 28 November 2017**

On 28 November 2017, the Article 29 Data Protection Working Party ("WP") adopted its "Guidelines on Consent under Regulation 2016/679" (the "Guidelines"). The WP invited public comments on this document. The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to submit the comments below.

In many instances, the Guidelines interpret and elaborate on the consent-related requirements of the General Data Protection Regulation ("GDPR") in a helpful way. For example, CIPL appreciates the express recognition by the WP that it is appropriate to provide information relevant to consent in layered format to accomplish clarity, precision and completeness. This is crucial, particularly in the context of mobile screens, given the amount of information required to be provided. CIPL also welcomes the recognition of both the "push" and "pull" models for providing information to individuals, though the "pull" model should receive even wider application than suggested by the WP, as further described below.

CIPL also welcomes the fact that the Guidelines clearly state that controllers have the flexibility to develop consent experiences that suit their organisation. Consent mechanisms are an integral part of customers' experience. It is, in fact, often the entrance door to the organisations services. Every organisation, depending on the service it provides and on its customers' experience, will have a different perspective on what an appropriate consent mechanism should look like. Organisations are also best placed to understand their audience and to foresee what type of consent mechanism is the most appropriate. Thus organisations must be granted flexibility in building consent mechanisms that meet the reasonable expectations of (1) individuals using their services and (2) regulators. The WP's final guidance on consent should enshrine this flexibility even more clearly.

However, CIPL believes that some aspects of the proposed Guidelines are not supported by the GDPR and will be unnecessarily burdensome and impracticable. As they stand, the Guidelines' interpretation of consent may limit the development of beneficial services for users, unnecessarily remove controller agency, and undermine the implementation of privacy by design. Indeed, some of the proposed implementation measures may have a

[1] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton & Williams LLP and is financially supported by the law firm and 59 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 & Williams.

negative impact on the protection and true empowerment of individuals, as well as on the digital economy, as further described below.

**Comments**

## I. Comments on the "Introduction to the Guidelines" (p. 4)

### A. The status of consent among "six lawful bases"

On page 4, the WP acknowledges that consent is only one of six legal grounds for processing personal data. However, it then goes on to say that "when initiating activities that involve processing of personal data, a controller must always take time to consider whether consent is the appropriate lawful ground for the envisaged processing or whether another ground should be chosen instead" (Emphasis added).

This statement should be reworded to avoid the suggestion that consent is the first "go to" ground for processing. This is not the case under the GDPR. Under Article 6 GDPR, no ground, including consent, is privileged over the other. Controllers are not required under the GDPR to consider whether consent is available for each processing activity, if another more appropriate basis applies.

Of course, to say that all processing grounds are equal as a matter of legal status does not mean that they must also be used with the same frequency. In the digital age, reliance on other processing grounds such as contractual necessity and legitimate interest must increase. This is especially true given the high threshold for valid consent under the GDPR. To avoid the risk of consent fatigue and thereby undermining the effectiveness and validity of consent where it is actually relevant in the modern information age, consent should be reserved for contexts where individuals can make meaningful choices about the processing of their personal data. CIPL agrees that individual empowerment and protection in the context of processing personal data is of utmost importance; however, consent is not the only way to achieve it.[2]

**Recommendation: Amend the above quoted sentence on page 4 of the Guidelines as follows: "When initiating activities that involve processing of personal data, a controller must always take time to consider the appropriate ground for processing. This may include considering whether consent is the appropriate lawful ground for the envisaged processing".**

### B. Consent under the ePrivacy Directive (p. 5)

On page 5, the WP addresses the issue of consent under the existing ePrivacy Directive and its possible replacement, the ePrivacy Regulation (EPR). CIPL agrees that this is an important

[2] CIPL has addressed the issue of consent under the GDPR in greater detail in its May 2017 White Paper "Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR", available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf.

issue, as it is essential that the notions of consent under the GDPR and the ePrivacy laws are in full alignment.

The issue of consent under the proposed EPR raises a wide range of problems that have been outlined extensively in CIPL's recent white paper on the proposed EPR [3] and in a separate study commissioned by CIPL on the impact of the proposed EPR.[4] The wide scope of application of the current proposal for an EPR , coupled with the high threshold for valid consent under the GDPR (as well as the absence of appropriate alternative grounds for processing under EPR, such as legitimate interest), compounds the problems associated with consent, as thoroughly discussed in the two papers. However, the final scope and content of a new EPR remains unknown. As a result, further discussion about the relationship between the GDPR consent requirements and the new EPR should be deferred.

**Recommendation: At this stage, given that the final scope and content of a new ePrivacy Regulation are still unknown, CIPL recommends that a discussion of how consent under the GDPR relates to consent under ePrivacy be deferred and addressed specifically in a wider context of how the GDPR will relate post May 2018 to the existing ePrivacy Directive (until the date when the new EPR is adopted and enters into force). The goal should be to align the two laws as to available processing grounds to ensure (a) consistent interpretations and applications of these processing grounds, (b) that the interpretation of the GDPR is not extended outside Personal Data, and (c) that the scope of the ePrivacy Regulation be appropriately limited to avoid diminishing the relevance and effectiveness of the GDPR, as described in the above mentioned papers. The WP should make a statement to that effect and undertake to clarify the relationship between the GDPR and ePrivacy Directive in a separate set of FAQs at a later date.**

## II. Comments on the "Elements of Valid Consent" (p. 6)

### A. Free/freely given (p. 6-7)

The Guidelines state that in order for consent to be valid, individuals must have a real choice and should not feel compelled to consent. The WP specifies that if the data subject is unable to refuse or withdraw consent without detriment, consent will not be considered to be valid.

Although it is clear from the GDPR that, in order to be valid, consent must be freely given, it is important that the WP take into account the range of different contexts and services where consent is sought when interpreting the meaning of "freely given" consent. Indeed, the concepts of "freely given" and "genuine choice" are not a one-size-fits-all and should be assessed taking into account the nature, scope, context and purposes of the processing. In practice, a range of approaches from a clear option to decline to engage with the company

[3] "Comments on the Proposal for an ePrivacy Regulation", 11 September 2017, Centre for Information Policy Leadership, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_proposal_for_an_eprivacy_regulation_final_draft_11_september_2017.pdf.

[4] "Study on the Impact of the Proposed ePrivacy Regulation", 19 October 2017, Niko Haerting, available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/epr_-_gutachten-final-4.0_3_.pdf.

or to leave or conclude receipt of a service, to the availability of more granular controls, may all safeguard individual choice without individuals feeling compelled to consent.

Specifically, regarding employee data processing, we agree with Example 5 provided on page 8 of the Guidelines. It would be helpful to include additional examples of "freely given" employee consents that involve situations with no negative consequences for employees who refuse to consent. Such examples of "freely given" employee consent might be:

- Consent of an employee in the context of subscribing to a fully optional share plan.
- A satisfaction survey that gives an employee the choice to respond or not to the survey (and consent to the data processing) or to answer the survey anonymously.
- Consent of an employee regarding activities that only marginally relate to the tasks of the individual in his or her capacity as an employee, e.g. the processing of his or her personal data when subscribing for the Christmas party or a charity event at work.

**Recommendation: Clarify that consent can be achieved through a variety of approaches and that, only where relevant, the availability of controls is an essential part in assessing whether consent is freely given. Provide additional examples of "freely given" consents in the employment context, as provided above.**

**B. Imbalance of power (p. 7-8)**

On pages 7 and 8, the Guidelines introduce some ambiguity by mentioning that apart from public authorities and employers, "other situations" may lead to imbalances of power. Legal certainty requires that these notions are clearly interpreted by regulators. Recital 43 of the GDPR only refers to public authorities. Controllers need legal certainty as to the definition of "imbalance of power", and the Guidelines should clarify the limited circumstances and high threshold to which they refer when noting "imbalances of power are not limited to public authorities and employers, they may also occur in other situations".

The WP refers to previous opinions and in particular to Opinion 15/2011 on the definition of consent.[5] This opinion focuses on data processing in the employment context and situations of subordination. The examples provided by the WP (e.g. body scanners, PNR, electronic ID cards) illustrate that emotional or practical detriment is a higher threshold than a mere disappointment or practical inconvenience of not being able to use a service.

**Recommendation: The WP should clarify what would constitute an imbalance of power outside of the cases of public authorities and employers. Specifically, the WP should emphasise that an "imbalance of power" would only occur in narrow situations where the individual truly does not have a meaningful opportunity to consent. Moreover, it should be confirmed that the popularity of a service does not impact and is not relevant to the**

[5] WP187 https://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

**validity of consent as defined in the GDPR, and that a cognisable imbalance of power requires a subordination situation. Finally, the concepts of deception, intimidation, coercion or significant negative consequences should be interpreted strictly. Deception should be understood as a material misrepresentation that has the effect of denial of access to a legal right or negative consequences that are similarly significant to the individual.**

### C. Conditionality (p. 8 and p. 10)[6]

An important issue relates to whether the assessment of the "conditionality" of consent under Article 7(4) prevents incentivising individuals to provide their consent with respect to processing of personal data that is "not necessary" for the performance of a contract. Article 7(4) is generally read to prohibit[7] conditioning the performance of a contract or provision of a service on consent to the processing of personal data that is not necessary for the contract or service. CIPL agrees that in many cases, under the GDPR access to a service may not be dependent on the consent of an individual for the use of his personal data for purposes which are not necessary for the contract or service. However, the GDPR allows that giving consent for these additional purposes may result in certain benefits to the individuals, such as additional service features or a lower fee. The WP should make this clear in its Guidelines.

CIPL agrees with the WP on the policy goal behind Article 7(4): "In general terms, any element of inappropriate pressure or influence upon the data subject [ ] which prevents a data subject from exercising their free will, shall render the consent invalid." However, CIPL believes that incentivizing an individual (such as by reducing the generally applicable fee or through another benefit, like a useful additional feature or service) to consent to additional processing should not be deemed to amount to "inappropriate pressure or influence" that "prevents" the individual from "exercising their free will." Thus, the WP should make clear that Article 7(4) does not preclude a controller from providing incentives, including additional benefits or financial incentives such as a discount from the generally applicable fee, if the individual consents to additional data uses that are not necessary for the performance of the contract.

Indeed, Article 7(4) provides for significant scope to incentivize individuals through cost differentiation and other means to consent to additional, beneficial processing of their data so long as there is no "inappropriate" pressure or influence and interference with free will. Moreover, without the ability to provide financial or other incentives such as discounts or

[6] In this section, CIPL discusses only the "conditionality" addressed in Article 7(4) relating to requesting consent for processing that is not "necessary" for providing the underling service. In Section III (Comment on Obtaining Explicit Consent) on page 14, we separately address circumstances where controllers must condition a "necessary" processing activity on explicit consent to the processing of special categories of data where other legal bases for processing are not available.

[7] According to the WP, there may be some "limited space for cases where this conditionality would not render the consent invalid." It also notes that under Article 7(4) and Recital 43, there is a presumption that conditionality will render consent invalid except in "highly exceptional" cases. Indeed, a less than categorical prohibition is suggested by the phrasing that – "utmost account shall be taken" of whether a service is "conditional." See Article 7(4)

other benefits, organisations might, in some contexts, be required to ask individuals to consent to processing without being able to provide a benefit in return. The WP should clarify this in its Guidelines. It should explain that a genuine choice of the data subject may exist in situations where consenting may lead to benefits, including financial benefits.

The statement regarding "no further costs" introduces a potential confusion, which the WP should clarify. For example, it is important to note that there are publishers, content providers, and service providers that rely exclusively on advertising to support their businesses. A standard that precludes any consequence or cost would effectively require a publisher to offer content without compensation. Many publishers exist only because they are funded by advertising; this is not unique to the online environment. Few publishers are state funded or not-for-profit, and subscriptions are not a viable alternative for all. Not allowing any financial benefits under Article 7(4) GDPR would threaten the existence of such publishers, content providers and service providers.

The standard is further confused by the choice of example at paragraph 3.1 of the WP's Guidelines: a "mobile app for photo editing" which users cannot use without consenting to, inter alia, use of personal information for behavioural advertising. The Guidelines note "the consent cannot be considered as being freely given" since the app cannot be used without consenting to this purpose. The WP should clarify that advertising services may be required to use such an app or service (given that many services are by necessity ad-supported), although the controller in the example may not require that an individual activate their GPS location services for behavioural advertising purposes to use the app.

**<u>Recommendation</u>: The WP should make clear that Article 7(4) does not preclude a controller from providing incentives, including additional service features or financial incentives such as a discount from a generally applicable fee, if the individual consents to additional data uses that are not necessary for the performance of the contract.**

### D. Granularity (p. 11) and Specific (p. 12-13)

On page 11, the WP states that consent must be granular to be considered as "freely given" and "specific" in accordance with Article 4(11). According to the WP,

> [a] service may involve multiple processing operations for more than one purpose. In such cases, the data subjects should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes. In a given case, several consents may be warranted to start offering a service, pursuant to the GDPR.

The WP also points out that according to Recital 43 "consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case". Quoting from Recital 32, the WP then suggests that one consent is possible as long as the processing activities serve the same purpose or purposes. This is corroborated by the language of Article 6(1)(a), which clearly states that consent may be given "for one or more specific purposes".

Nevertheless, the WP then includes an example (Example 7) that appears to contradict this principle:

> Within the same consent request a retailer asks its customers for consent to use their data to send them marketing by email and also to share their details with other companies within their group. This consent is not granular as there is no separate consents for these two separate purposes therefore the consent will not be valid.

The practical application of this interpretation of granularity presents several challenges for businesses. In particular, in Example 7, data sharing with affiliates should be considered as a processing operation – not as a separate purpose – if it forms part of the processing aimed at marketing (marketing being the purpose of processing). Providing separate consents for different processing activities under the same purpose (as shown in Example 7 above) could cause "consent fatigue". This creates two possible outcomes, both of which are potentially detrimental to the individual and organisations alike:

- Making consent meaningless, as individuals would just click to get to the service they want to receive as soon as possible. This would undermine the primary goal of the GDPR, namely to provide individuals with genuine control over the use of their personal data.

- Leading individuals to "over refuse" their consents, which would have a negative trade impact on businesses across Europe and undermine the ambition of the EU Digital Single Market.

This interpretation of the granularity requirement could also prove challenging in organisations that have different companies that may be pursuing a common group purpose but through slightly different activities - for example, a retail group may have several different companies selling different products or services. If the common pool of data is managed centrally, this would potentially mean that individuals have to provide granular consent for different processing activities under the same purpose. Similarly, where purposes for processing are related, conceptually similar, or technically dependent on each other, it will be clearer, more informative, and more sensible for the individual to provide consent to those multiple purposes together. Thus, for groups of related purposes, and where appropriate information is presented to users, it should be valid and appropriate to have one "consent moment", together with appropriate revocation mechanisms. Such an approach is more in line with a user-centric interpretation of the GDPR (clear, concise and not necessarily disruptive (per Recital 32)) and would avoid that users suffer from consent fatigue.

**<u>Recommendation</u>: Take a flexible approach with respect to the interpretation of "granularity." This would allow organisations to ensure that the reasonable expectations of individuals are respected by giving them control over the use of their data through clear and concise privacy notices and "just in time" notices but without necessarily the need to obtain consent for each processing activity that is aimed at the same or linked purpose(s), or for each processing activity that is intrinsically linked with another. Thus, granularity and specificity can be better served by: (1) appropriate information on related data processing purposes; (2) clear means of refusal, revocation or control in respect of the data processing and, (3) where appropriate, one "consent moment" for a group of related**

**purposes. Example 7 should be revised to reflect that individuals should be clearly informed that marketing operations are carried out jointly by all the businesses belonging to the same group with more information about group companies in a sub-layer of the notice, as well as how to withdraw consent.**

### E. Detriment (p. 11)

On page 11, the WP states that "the controller needs to demonstrate that it is possible to refuse or withdraw consent without detriment (Recital 42)". The WP goes on to state that withdrawing consent should "not lead to any costs for the data subject" or to any "clear disadvantage for those withdrawing consent." The WP should clarify that a withdrawal of consent that leads to detriment is possible only where an individual withdraws consent with respect to processing not necessary for the underlying contract or service and such withdrawal impacts the main or underlying service the individual originally consented to.

Moreover, in certain situations, consent will be the only legal basis for a controller to process personal data, such as with sensitive personal data where an organisation needs to process biometric data as an integral part of the service. If consent then is withdrawn, the organisation cannot perform the required biometric data processing, and hence cannot continue to offer the service to the individual. For example, where facial recognition is used to check the photo in a passport against the photo on an account as part of fraud prevention checks, or where an organisation might ask an individual to take another picture to compare against the one on the account before taking specific actions, such as deleting the account or authorising the purchase of age-restricted items. Thus, the WP should clarify this section so as to not capture these types of activities that will have to stop when consent is withdrawn.

As mentioned above, where an individual withdraws consent to processing that is not necessary for the underlying service and such withdrawal affects the main or underlying service the individual originally sought, such impact on the underlying service may be deemed a detriment to the individual as per Recital 42 of the GDPR.

The Guidelines note on page 11 that "[i]f a controller is able to show that a service includes the possibility to withdraw consent without any negative consequences e.g. without the performance of the service being downgraded to the detriment of the user, this may serve to show that the consent was freely given" (Emphasis added). The WP's primary concern relates to a downgrade or "detriment" with regard to the underlying service.

Where consent for an "unnecessary" additional processing activity was incentivized by reducing the fee for the underlying contract or service, reinstating the full fee upon withdrawal of the consent should not be deemed a detriment, cost or disadvantage to the individual that would violate Article 7(4).

Thus, CIPL believes that WP should clarify that in determining "detriment" the focus should be on whether, upon the withdrawal of consent for an "unnecessary" processing activity, the underlying service is somehow unnecessarily downgraded (in its quality, or basic scope, for example), and not whether there was a financial consequence as a result of lifting a discount or other financial incentive for the initial consent for the "unnecessary" service.

In addition, it must be made clear that there may be "downgrades" to the service that are unavoidable, such as where the (withdrawn) consent to the data processing was necessary for additional functionality or features that will end with the withdrawal of consent. In such cases, there would not be a "downgrade" of the service amounting to "detriment" for purpose of establishing whether Article 7(4) is violated, as the features affected do not detrimentally affect the main or underlying service the individual originally consented to.

For the avoidance of doubt, WP should clarify that the following situations do not constitute a "detriment" to individuals:

- Failure to provide the individual with any additional benefits/advantages created by and/or inherently linked to the data processing to which the individual declined to consent;

- Mere inconveniences and/or disappointments which do not materially affect the individual's legal rights and positions.

Moreover, refusing to enter into arrangements or ceasing the service should clearly be distinguished from the "downgraded performance" situation mentioned in the WP's guidance for the following reasons:

- A "downgraded performance" assumes that a services is being provided. When the use of a service is terminated (or not even begun), a company is generally not entitled to process personal data and thus cannot "downgrade" any performance.

- An example of "downgraded performance" could be the case where a "standard service" is provided to an individual based primarily on alternative legal bases to consent, for example, contractual necessity and legitimate interest, with the availability of a few additional features based on consent. By refusing consent to the few additional features, an individual would not be considered as receiving a "downgraded service" (i.e. the "standard service" absent the extras) *unless* that "standard service" was additionally degraded in some manner by the controller in reaction to the refusal / revocation of consent (e.g. the "standard service" would be caused to run slower, or the individual's experience would be presented differently, for example with lower resolution).

**Recommendation: The WP should clarify that "detriment" only applies to withdrawal of consent with respect to processing not necessary for the underlying contract or service that results in a detrimental impact to the main or underlying service. In addition, where the consent was incentivised and the withdrawal of consent results in reversing the benefits of the incentive, such reversing of the incentive should not be deemed a "detriment." Further, the WP should include the above examples of what is not a "detriment" and of what does or does not constitute a "downgraded performance." Finally, where processing is based on consent, the guidance should acknowledge that there is no "detriment" if no service is provided or the service is stopped where the individual refuses to give consent or withdraws consent.**

**F. Specific (p. 12)**

On page 12, last paragraph, the WP states the following: "The original consent will never legitimise further or new purposes for processing." This statement should be qualified and address further processing that is allowed under the GDPR (e.g. Articles 5(1)(b) and 6(4)).

**Recommendation: Amend the last sentence in the final paragraph on page 12 (before Example 8) as follows: "The original consent will never legitimise further or new purposes for processing, unless permitted under the GDPR."**

**G. Informed (p. 13 and p. 16)**

CIPL welcomes the WP's recognition on page 14 that the GDPR does not prescribe any specific format for information to be provided to individuals, and that layered notices are presented as an appropriate way to solve the two-fold obligation of being precise and complete on the one hand, and understandable on the other hand. We also welcome the fact that the WP acknowledges on page 15 that not all elements of Article 13 and 14 always have to be provided in the process of obtaining consent, provided they are given in other places, e.g. in the privacy notices, policy or elsewhere.

On page 14, the WP notes that there should be a clear separation between information related to obtaining consent for data processing activities and information concerning other matters. It should be clarified that although it should be easy for an individual to identify directly what information relates to the consent sought and what information concerns other issues, in many cases it is important for an individual to have a broader picture to exactly understand to what he or she consents to and the context of other related data processing which may be undertaken on an alternative legal basis. It may be important for the individual to understand that, even if he or she does not consent to certain data processing, for example, the same type of data may be used for other purposes pursuant to another legal basis than consent. Presenting such information up-front during the consent procedure may be an appropriate way to safeguard transparency and fairness for the broader processing undertaken.

**Recommendation: The guidance should recognise that, in some cases, it may be important to include information about consent in context with other information in order to provide a full picture to the individual and safeguard transparency. It should be clear what information relates to the request for consent, and what information relates to other topics.**

The WP also points out on page 13 that the identity of the controller must be identified to obtain valid/informed consent. And on page 14, it states that in the case of multiple (joint) controllers, "these organisations should all be named." This requires further clarification.
Indeed, the Guidelines acknowledge that clear, concise, and plain language is important for informed consent, and that layered information can be an appropriate way to be both precise and understandable, especially to accommodate for small screens or situations with restricted room for information. Thus, in the case of multiple (joint) controllers, a long list of corporate entity names would not be particularly helpful to an individual (and would take

crucial attention away from other key aspects of the consent, like the purpose of the processing).

**Recommendation: Clarify that information about multiple (joint) controllers should be presented in plain and simple language and in a manner that appropriately informs the data subject (e.g., with a secondary layer including additional detail or examples).**

On page 14, the WP recommends a layered approach to address the tension between (1) the need for information that is relevant for the individual to make an informed decision on consent and for it to be clear and concise and not buried in general terms of use and (2) not being "unnecessarily disruptive" in requesting consent. As noted previously, CIPL appreciates the recognition of the value of providing information in layers. The level of detail in each layer will affect how helpful and clear the information is. For example, on page 13, the WP identifies six elements that are required to obtain informed consent. If each of those is provided in the top layer, the consent experience could result in a wall of text, especially on small mobile screens. It would be helpful for the WP to clarify that the top layer can be designed to provide more limited information, such as the type of data and the purposes of the processing, provided it links directly to another layer, such as a privacy statement, that includes the remaining information and may include the additional elements required by Articles 13 and 14.

**Recommendation: The WP should make clear that the information listed on page 13 as required for obtaining valid consent may be provided in a combination of the top layer of information plus a privacy statement or other more detailed – but still clear and concise – layers.**

### H. Unambiguous indication of wishes (p. 16)

The GDPR requires that consent be expressed by a clear affirmative act. We welcome that the WP acknowledges that this should not be unnecessarily disruptive to the use of the service for which consent is provided (as per recital 32) and that companies are free to develop a consent mechanism that suits their organisation. Indeed, the expression of consent can take various forms and should be assessed in the context of the entirety of the individual experience.

The WP notes on page 16 that "merely proceeding with a service" cannot be regarded as an active indication of choice. It should be clarified that by "merely proceeding with a service" refers to situation where no affirmative action is taking place at all. On the other hand, filling in a free-text field, for instance as part of the creation of a profile that is necessary to the use of an online service, or clicking a button to accept a set of options, service configuration, or settings should be considered as a valid affirmative (and explicit) action to the extent that the individual is provided with relevant and appropriate prior information, and that it is clear to him/her that by filling in the information he/she expresses consent.

**Recommendation: The WP should clarify that completing a free-text field and other similar actions, in certain circumstances (including with reference to any information provided to the individual), may constitute a valid (and indeed explicit) affirmative act.**

On page 17, the Guidelines state that "[t]he GDPR does not allow controllers to offer pre-ticked boxes or opt-out constructions that require an intervention from the data subject to prevent agreement (for example 'opt-out boxes')." CIPL suggests that the WP provide a more nuanced discussion of the type of "opt-out" it intends to preclude because not all opt-out constructions fit this characterisation.

For example, the WP refers in a footnote to its "Working Document 02/2013 providing guidance on obtaining consent for cookies."[8] This document includes the following relevant statements in relation to consent:

> Active behaviour means an action the user may take . . .[9]
>
> Ensuring that the button, link or box which indicates the active behaviour is within or close to the location where information is presented is essential to be confident that the user can refer the action to the information prompted.[10]
>
> The user action must be such that, taken in conjunction with the provided information on the use of cookies, it can reasonably be interpreted as indication of his/her wishes.[11]
>
> The users should have the opportunity to freely choose between the option to accept some or all cookies or to decline all or some cookies and to retain the possibility to change the cookie settings in the future[12] (Emphasis added).

The above language would allow "decline" mechanisms to indicate consent for certain processing which, together with other actions by the individual, ensure that the controller knows whether the individual has shown agreement with the processing at hand. This means, for example, that a box saying "No, I don't want you to process my personal information for this purpose", or a "No" box for each purpose and a requirement of a signature at the end of the document, may be considered as unambiguous consent if there is clear and transparent information about each purpose.

Opt-out mechanisms linked with other means that allow indication or declaration of agreement by the user, should not be excluded from the available techniques used to obtain an unequivocal or unambiguous consent, provided that the necessary guarantees are given so that such consent is understood to be validly granted (such as clear and specific information on the processing at hand and the possibility of revoking consent).

Further, while Recital 32 is clear that silence, pre-ticked boxes, or inactivity do not alone constitute consent, the text of the GDPR allows controllers to abide by principles of privacy by design to establish appropriate defaults for data collection and processing. Thus, we do not agree with the WP's statements that "the use of pre-ticked opt-in boxes is invalid under

[8] Working Document 02/2013 providing guidance on obtaining consent for cookies, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf.
[9] Id. at p. 4.
[10] Id.
[11] Id. at p. 5.
[12] Id.

the GDPR" (p. 16) and "the GDPR does not allow controllers to offer pre-ticked boxes or opt-out constructions that require an intervention from the data subject to prevent agreement" (p. 17). A controller should be able to propose default options that require the individual to either affirmatively indicate agreement or to decline or modify the option. Requiring that all data collection and processing options be off by default across all services would increase click fatigue, impair user experience and service functionality, and limit controllers' design freedom.

**Recommendation: Provide a more nuanced discussion of "opt out", acknowledging that certain mechanisms that might be characterised as "opt out" nevertheless meet the GDPR "unambiguous" consent requirement, such as where it is accompanies by additional actions indicating consent. Also clarify that while pre-ticked opt-in boxes will not alone constitute consent, where the consent requirements are otherwise met (e.g., by the inclusion of a separate mechanism to indicate agreement), an appropriate default may be used.**

### I. Consent through electronic means (p. 17)

On page 17, the WP acknowledges the risk of "click fatigue" associated with the way legislators drafted the GDPR's consent requirements. However, rather than offering meaningful, actionable guidance, the WP essentially refers the problem to controllers: "The GDPR places upon controllers the obligation to develop ways to tackle this issue."

CIPL supports the GDPR concept of accountability of organisations, which coupled with the risk-based approach requires controllers to determine the best compliance strategies and methodologies. However, the consent fatigue problem cannot be solved only by refining the available consent strategies, flows and mechanisms. This goes back to the issue raised above in Section I. A: to avoid undermining the effectiveness of consent where it is truly needed and appropriate, it must be permissible to use consent sparingly and only where it truly adds to the empowerment and protection of the individual in ways that other processing grounds cannot. It is these policy choices and steers by the data protection authorities that can also impact users' experience and compliance in the marketplace and avoid creating consent fatigue and privacy-indifferent users. Thus, CIPL urges the WP to confront the problem of click and consent fatigue head-on by acknowledging the need to apply alternative bases for processing, particularly contractual necessity and legitimate interests, wherever they are appropriate and applicable.

**Recommendation: Acknowledge the inherent tension between extensive reliance on "valid consent" and consent fatigue and that in the modern digital economy the burdens of frequent consent requests may be unavoidable and cannot be overcome solely by refining consent mechanisms. Acknowledge that Data Protection Authorities and organisations both bear responsibility to find solutions to this problem. One part of the solution must be a policy of recognising and accepting the appropriate use of alternative grounds for processing whenever possible.**

Recognizing the risk of click fatigue, the WP suggests relying on browser settings, which it says on page 17 should be developed to support GDPR consent, including per-purpose and informed consent. Absent standards to address the exchange of information and signals

between controllers and the browser and enforcement against controllers that purport to rely on a third party's browser settings without providing the necessary information or respecting to-be-determined signals, the browser will have neither the names of controllers nor any of the other required information to provide to individuals. Browsers are by nature global tools that should not be expected or encouraged to mediate legal compliance in the EU for unrelated controllers. And since requests for consent will occur frequently with or without browser settings, the proposal would fail to address click fatigue. CIPL recommends that the WP delete the last paragraph on page 17.

**Recommendation: Remove the final paragraph in Section 3.4.1 on page 17 ("Consent through electronic means").**

## III. Comments on Obtaining Explicit Consent (p. 18)

On pages 18 to 19, the WP addresses the issue of "explicit consent" required by the GDPR in the context of special categories of data, certain transfers to third countries, and automated decision-making. The WP suggests that explicit consent will require more of an express action on the part of the individual to grant his or her explicit consent than "ordinary" consent would. Examples for such additional express actions provided by the WP include two-factor verification, electronic signatures, signed statements, email verification, and the like.

Such measures require collection of data beyond that which may be necessary for the processing. Additionally, in the context of a mobile application, such measures would be burdensome for the individual, as he or she would be required to potentially interact outside of the confines of the application itself to choose to consent to processing of his or her data. For example, health and wellness monitoring devices with companion applications are increasingly common. An individual may wish to upload the data gathered by his or her device, which may include heartrate or blood pressure measurements, to a server-based application (via a mobile application or some other mechanism) that will store and process the data on his or her behalf and allow the user to make better use of the data and monitor his or her wellness. Due to the inclusion of sensitive categories of data, explicit consent is the only lawful basis of processing. However, the individual may not have been asked to share his or her actual name, email address, or any of the other information that would be required for mechanisms such as electronic signatures or email verification, because this may not have been necessary for the processing (and, as such, under the tenet of data minimisation, would not have been collected). It would be difficult or impossible to build in these additional mechanisms without collection of further data.

Also, affirmatively clicking a button that says "I Consent" or otherwise clicking to accept an explicit consent statement after being presented with all relevant information about the proposed processing requiring express consent (and then, possibly, clicking "Continue") is an express indication that the individual wishes to move forward with the processing and should be recognised as such in the Guidelines.[13] However, the WP seems to suggest that

[13] The ICO consultation on GDPR consent provides a more practicable standard for obtaining explicit consent. It supports offering the user an "explicit consent statement" that can be accepted. The practice includes a statement saying "I consent to [processing requiring consent]," and then if the individual clicks on a button or

may be insufficient, even though it is an explicit action taken by the individual, which could be demonstrated fully by the controller's records. Individuals would be burdened by the requirement to submit some additional form of affirmative consent, such as a signed statement or verification through email.[14] Moreover, there would be no additional advantage to such measures in many contexts. As such, these measures may be disproportionate to the need, which is just to ensure that the individual is making a conscious, informed, express decision to grant the consent and that this can be demonstrated by the controller.

Also, mechanisms for dual-factor verification, electronic signature, and others may require significant development efforts, which would be difficult or impossible in the short timeframe left between the issuance of the finalised Guidelines and 25 May 2018, especially for SMEs and start-ups.

Finally, by focussing on the expression of consent, the WP does not cover the most important rationale underpinning "explicit consent", which is that the individual should understand that special categories of data may be processed, or that their data may be transferred outside of the European Union to countries that do not have similar legal regimes, and the implications of this. The WP rightly points out that "normal" consent in the GDPR is now raised to a higher standard compared to the Directive by requiring an affirmative act. It follows that the principal distinction between 'standard', and explicit, consent should lie in the information provided to the individual, rather than in the manner or form in which consent is expressed. This is clearly demonstrated as the will of the legislature in the framing of 'explicit' consent in the context of transfers, with Article 49(1)(a) requiring that, individuals are "*informed of the possible risks of such transfers*".

**Recommendation: The WP should acknowledge a more nuanced picture with respect to how explicit consent may be implemented in a wide range of contexts. Importantly, there should be no automatic presumption that the requirements of "explicit consent" have not been met where controllers applied the requirements for "regular" consent under the GDPR. Where "regular" consent is already "explicit" due to the nature of the unambiguous indication in a statement or affirmative action, and the consent mechanism/procedure provides specific information about the data processed and the potential associated risks/implications of the data collection/processing, the requirement of "explicit" consent under Article 9(2)(a) may already be fully met. Explicit consent should simply mean that the consent was explicit (clear; express), based on heightened information provided to the individual, and that it was demonstrably so. The examples**

---

ticks a box, she will have explicitly consented to the processing. The WP should consider suggesting this approach in the Guidelines as well. See ICO consultation on GDPR consent guidance, March 2017, p. 25 https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf.

[14] Indeed, having an online/digital form or app that has two, three or more opportunities for the individual to provide their consent ("do you consent?", "are you sure?", "are you sure you're sure?) is functionally no different from dual-factor verification, just less burdensome for all involved. Perhaps the WP assumes that dual-factor involving different media (email, weblink, SMS) ensures an individual is making an informed decision since they are less prone to blindly click through an app or website. But it is likely to have the opposite effect by imposing hurdles that deter an individual.

**provided by the WP may be useful and appropriate in some contexts but may not be necessary in other contexts. For example, the WP should acknowledge that affirmative actions, such as (1) ticking a consent box; and (2) subsequently clicking a "continue" button, may meet the requirements of explicit consent, provided the information to individuals includes the specific aspects and circumstances requiring heightened, explicit consent.**

On page 19, in the context of discussing how to provide explicit consent, the WP notes that explicit consent is not the only way to legitimise the processing of special categories of personal data, pointing out that there are eight additional legal grounds. However, it should be noted that those options are very narrow and will not provide a legal ground for most organisations and in most contexts. This means that in reality there will be very limited options for the legitimate processing of special categories of data, in most cases, requiring explicit consent. However, even that option is potentially severely restricted under the GDPR, if the WP's interpretation of the explicit consent requirement is more restrictive than necessary and may prevent some legitimate cases of processing of sensitive personal data, not covered by other legal grounds.

For example, contractual necessity will not be available to controllers for special categories of data and in most cases controllers will need to rely on explicit consent. Thus, where a controller wishes to process biometric data that are necessary to access and power the service, it will have no other choice but to consider that if a user does not consent to this processing, the controller will not be able to provide the service. The guidance should clarify this issue by saying that in some cases conditionality would not render consent invalid. This means that in some situations a "take it or leave it" approach should be possible and specific examples should be offered in this respect in order to ensure clarity and legal certainty.

Another example would be where an employer procures health insurance coverage for its employees and each employee will need to log into the service and enter his or her information, which will include health information through various background screening questions (e.g., do you smoke, how much alcohol do you consume, have you had prior surgeries, etc). If the employee does not consent to give this information he or she cannot get insurance and as such the consent is conditional. There is simply no alternative to collecting this information.

A further example could be processing of biometric data for fraud prevention. Some countries (like the UK) have introduced a lawful basis for processing sensitive data for fraud prevention purposes. However, even if this is seen as a public interest in other countries, the absence of a similar lawful basis in a country's data protection or other law may mean companies have no choice but to use explicit consent instead. Indeed, the absence of a specific provision in a country's data protection or other relevant law to the effect that certain processing is necessary for substantial public interest (consistent with Article 9(2)(g)) may also impact other "pubic interest" processing of special categories of data.

**<u>Recommendation</u>: Clarify that in certain cases involving sensitive categories of data where explicit consent is sought, there may be an element of conditionality where there are no**

**other viable options beyond consent. Thus, the WP should acknowledge that when a data processing is necessary for a controller to provide its service and contractual necessity is not an available legal basis (e.g. special categories of data), a controller should be able to condition the service on consent or take a "take it or leave it" approach for the service or part of the service. Moreover, in situations where special categories of data are part of a feature or service, clarify that an individual may expect that he or she will not receive the part of the service that is based on the processing of sensitive personal information if he or she has not consented to this processing. Finally, clarify how processing of special categories of personal data for fraud prevention (or other public interest purposes) should be handled in the absence of a special national legislation under Article 9(2)(g).**

## IV. Comments on "Additional conditions for obtaining valid consent" and on "Interaction between consent and other lawful grounds in Article 6 GDPR" (p. 20 and p. 22)

### A. Demonstrate consent (refreshing consent) (p. 19)

On page 20, the WP correctly states that the GDPR does not impose specific time limit for duration of consents, noting that the only criterion in the GDPR is that a consent is no longer valid if the processing operations "change or evolve considerably", in which case a new consent must be obtained. Notwithstanding this clear articulation of when a new consent is required, the WP goes on to say that, as a matter of "best practice [ ] consent should be refreshed at appropriate intervals".

This recommendation is problematic. Not only is this not required and adds no value if the processing has not changed or evolved significantly, it raises the questions of whether, by what criteria, and for what purpose this "best practice" would be evaluated by data protection authorities. Moreover, it imposes unnecessary burdens on organisations and individuals who, at any given time, will receive requests to refresh consent from many different services, resulting in an ongoing stream of consent requests and subsequent consent fatigue. CIPL recommends that the WP remove this recommended best practice.

**Recommendation: The WP should delete the "best practice" recommendation that consents should be periodically refreshed even where the relevant processing operations have not changed. Such refreshing is not required by the GDPR and would impose significant burdens both on organisations and individuals.**

### B. Withdrawal of consent (p. 21)

On page 22, the WP states that ". . . if consent is withdrawn . . . [i]f there is no other lawful basis justifying the processing (e.g., further storage) of the data, they should be deleted or anonymised by the controller" (Emphasis added). It also states that "[b]esides controller's obligation to delete data that was processed on the basis of consent once that consent is withdrawn, an individual data subject has the opportunity to request erasure of other data concerning him that still resides with the controller, e.g. on the basis of Article 6(1b)" (Emphasis added).

We do not believe that it would be logical to a user that his or her data would be automatically deleted upon revocation of consent. Two examples are provided below as use cases wherein this would potentially cause issues or confusion:

- An individual may have given consent to automatic uploads of pictures taken from his or her mobile device to an online cloud storage solution, and no other lawful basis for the processing is applicable. This individual may decide that he or she no longer desires to automatically upload his or her pictures to this repository and revoke his or her consent so that the automatic uploads cease. This does not necessarily mean that the user does not want to continue storing previously uploaded images in this repository. To assume otherwise would be a detriment to users who wish to keep their previously uploaded images in the repository. Other users wishing to also delete the previously uploaded photos could just submit a data erasure request to have them deleted.

- An individual may have given consent to upload his or her health-related information, such as blood pressure measurements, heart rate measurements, or other sensitive data" to a server-based solution which stores and analyses such data on his or her behalf. This individual may desire to discontinue uploading such data going forward and revoke his or her consent for such future uploads; however, the individual may still wish to have historical data, previously uploaded, stored for future viewing, export, or review.

In both examples, under the Guidelines, automatic deletion of the data would be required if no other lawful basis for continued storage exists. In the case of sensitive categories of data, organisations normally do not have any other lawful bases for processing other than explicit consent. We believe this interpretation to be inconsistent with the text of the GDPR and detrimental to individuals in at least the following respects:

- Obliging the controller to automatically exercise the individual's right of erasure upon revocation of consent is contrary to the intention in the GDPR to allow the individual to have control over his or her data and its use. The GDPR requires that users be able to decline/revoke consent without detriment (Recital 42). If a revocation of consent triggers deletion of the data, this would certainly result in negative consequences for the user in the form of data loss and loss of individual rights, such as portability. The intention to revoke consent for future processing does not by default signify an intent to delete all previously processed data.

- The upload and storage of data is intrinsically linked on the front end. If you upload the data, but then cannot store it, the consent to upload is meaningless. The converse is true as well. Requiring such granular consents as Consent #1 to upload the data, Consent #2 to save the data to the server, Consent #3 to perform some processing on the data (such as storage), and so on would be confusing to the user (as well as burdensome), as some of these actions are impossible without consent to the prior action. Once the data has been uploaded, it is then separated and the user

may perform activities specifically on that data, such as to rectify inaccuracies or delete it altogether. It has been decoupled from the upload process. As such, a later revocation of the consent would not logically revoke consent to store the data, but only to upload future data. Withdrawal of consent is not an "undo" action; it is an affirmative choice for future processing.

- Scientific research: Data collected must be maintained in order to guarantee the quality, integrity of data and of the results. Individuals who have provided their consent, even after withdrawing such consent for future use, have an intrinsic and vested interest in the ability of the controller to achieve reliable results and make relevant scientific inferences and linkages, including for safety reasons.

- Clinical Trials: The Clinical Trial Regulation, which will enter into force in 2019, clearly states (Recital 76 and Article 28(3)), that: "With a view to respecting those rights, while safeguarding the robustness and reliability of data from clinical trials used for scientific purposes and the safety of subjects participating in clinical trials, it is appropriate to provide that, without prejudice to Directive 95/46/EC, the withdrawal of informed consent should not affect the results of activities already carried out, such as the storage and use of data obtained on the basis of informed consent before withdrawal".

**Recommendation: Clarify that withdrawal of consent should not automatically result in the deletion of the data that was previously processed pursuant to the consent, as such deletion may be contrary to the individual's expectations and wishes. In addition, the deletion may interfere with the exercise of other GDPR rights and may be in conflict with other regulations, such as clinical trials and scientific research.**

**C. Withdrawal of consent and Interaction between consent and other lawful grounds in Article 6 GDPR (p. 21 and p. 22)**

On page 22, the WP also states that after withdrawal of consent, the controller who wishes to continue processing cannot "silently migrate from consent (which is withdrawn) to [another] lawful basis. Furthermore, any change in the lawful basis for processing must be notified to the data subject in accordance with the information requirements in Articles 13 and 14 and under the general principles of transparency (Emphasis added).

CIPL takes the view that, indeed, when an individual revokes his or her consent the processing generally cannot just continue based on another legal ground without the individual being informed and able to act.

The WP should affirmatively state that if consent is withdrawn and another processing ground applies, and the conditions for the validity of the latter are met (including the information that must be provided under Articles 13 and 14 GDPR), then the controller may continue to process data. The controller must respect appropriate notification and transparency requirements or must have anticipated this alternative ground in the initial notice.

There are several arguments in support of CIPL's view:

- Article 17 (erasure) envisions just this very process of continuing with another legal ground where consent is withdrawn. Article 17(1)(b) states that data must be erased where "the data subject withdraws consent on which the processing is based . . . and where there is no other legal ground for the processing" (Emphasis added).

- The WP suggests for good reasons that processing based on an alternative ground may continue if applicable notification requirements of Article 13 and 14 are complied with.

- The WP also states on page 23 that "[b]ecause the requirement to disclose the lawful basis which the controller is relying upon at the time of collection of personal data, controllers must have decided in advance of collection what the applicable lawful basis is." However, the position that a processing activity must be based on one, pre-determined legal basis and cannot be based on multiple lawful bases is incompatible with the text of Article 6 GDPR whereby "[p]rocessing shall be lawful only if and to the extent that at least one of the following [legal grounds] applies: [ ]" (Emphasis added). The expression "at least" means there can be multiple legal bases for one processing.[15]

- A position that the lawful basis cannot not be modified in the course of processing also conflicts with two practical scenarios where flexibility should be expressly given to the controller, because consent can be combined with another legal basis:

(1) When a processing based on legitimate interests is "extended" over time, it could be reinforced by consent.

In this case, the purpose of processing would remain the same, as would the individual(s) and controller(s), but, at one point in time, the data would be distributed to more recipients and/or would be stored longer than disclosed originally, and/or would reach more non-adequate countries. Such modifications would normally not affect the legitimacy of processing the data, but they may nevertheless alter the balance with the individual's own interests and privacy expectations. Indeed, when looking at WP Opinion 06/2014 on the notion of legitimate interests, we see that the balancing test should "take into account the way data are processed (large scale, data mining, profiling, disclosure to a large number of people or publication)" as well as "data minimisation [measures] (e.g. strict limitations on the collection of data, or immediate deletion of data after use)".

Accordingly, it would be appropriate to allow controllers to further legitimise their processing by providing updated information to individuals and requesting their express

[15] The ICO Guide to the GDPR also supports the idea that multiple legal bases may apply, on the condition that the data subject is being informed from the start: "It may be possible that more than one basis applies to the processing, and if this is the case then you should make this clear from the start" ICO Guide to the General Data Protection Regulation, at p. 14, available at https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf.

assent to carry-on under the modified conditions. If the consent is denied, the data processing could be pursued under the former conditions; if the consent is granted, the data processing could be pursued under the new conditions, with a new legal basis.

(2) In the context of cross-border processing, especially within multi-national organisations, the correct legal basis may vary between countries.

A good example of such variation of legal grounds concerns the disclosure of remunerations paid by pharmaceutical companies to healthcare professionals. The EFPIA (European Federation of Pharmaceutical Industries and Associations) has been conducting studies on the legal bases for such a processing of personal data under the Directive and under the GDPR. The EFPIA has established that three separate legal bases could be used, depending on the countries: the respect of a legal obligation (e.g. France or Denmark), the legitimate interests of the controller (e.g. Spain or the Netherlands), or the consent of the healthcare professional. If a multi-national company organises a conference for healthcare professionals from different European countries, this company will need to verify each time the appropriate legal basis, which may vary from one country to another and over time and apply different legal bases for its disclosure of remuneration paid to the healthcare professionals depending on in which country the company and/or the healthcare professional are based. Accordingly, a fair and practical solution for cross-border processing would be to allow processing on alternative grounds, whichever is applicable under the applicable law.

**Recommendation: Clarify that it is possible to have multiple legal grounds for one and the same processing. Also, the WP should affirmatively state that if consent is withdrawn and another processing ground is available, and the conditions for the validity of the latter are met (including the requirements of articles 13 and 14), then the controller may continue to process data.**

## V. Specific Areas of Concern in the GDPR (p. 23)

### A. Children (Article 8) (p. 23)

Article 8 relating to children's data raises a wide range of complex compliance issues, some of which are discussed by the WP. However, CIPL does not address these issues in the present comments. Instead, CIPL intends to convene a multi-stakeholder event to initiate a policy dialogue on the these issues and then to prepare a separate white paper or commentary on all issues relating to Article 8, including the issues of age verification, verification of parental responsibility, information society services directed to children, and other GDPR requirements relating to children.

### B. Scientific research (p. 27)

The WP's narrow definition of scientific research on pages 27-28 is at odds with Recital 159, which makes it clear that "scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research" (Emphasis added). In addition,

this is an area where Member States have margin of manoeuvre, hence the WP should not be this restrictive, as the interpretation risks conflicting with national laws. For example, during the Parliamentary readings on the UK's draft Data Protection Bill, there has been significant time devoted to discussing the provisions on scientific research and proposing amendments to make sure it is not unduly restrictive. Specifically, in relation to a proposed amendment relating to biometric data processing the debate transcript quotes a Government letter that stated:

> "You also queried whether researchers involved in improving the reliability or ID verification mechanisms would be permitted to carry on their work under the GDPR and the Bill. Article 89(1) of the GDPR provides that processing of special categories of data is permitted for scientific research purposes, providing that appropriate technical and organisational safeguards are put in place to keep the data safe. Article 89(1) is supplemented by the safeguards of clause 18 of the Bill. For the purposes of GDPR, 'scientific research' has a broad meaning. When taken together with the obvious possibility of consent-based research, we are confident that the Bill allows for the general type of testing you have described."[16]

This quote, and the subsequent parliamentary debate, make it clear (a) that while consent may be a possibility in some research contexts, it by no means works in all contexts, such as in the context of R&D, where reliable results depend on solid data sets in terms of volume and type that cannot be left to individual choice; and (b) that the broad range of "scientific research" should extend to private sector R&D.[17]

**<u>Recommendation</u>: Add the remaining wording from Recital 159 that is missing in the quote on page 27 to make clear that scientific research goes beyond medical research and encompasses private sector R&D. Delete the phrase ". . . however the WP29 considers the notion may not be stretched beyond its common meaning and understands that 'scientific research' in this context means a research project set up in accordance with relevant sector-related methodological and ethical standards [ ]" and replace it with: "The WP29 considers the notion should not be unduly stretched and 'scientific research' in this context should follow relevant sector-related methodological and ethical standards where these are available."**

In addition, the WP's recommendation with respect to transparency as "an additional safeguard when the circumstances of the research do not allow for a specific consent" is not a solution where the object of the research is fraud prevention and the interface is a mobile screen. Much of the R&D use for fraud prevention cannot be disclosed to individuals who might use them to circumvent such anti-fraud measures. Thus, complete transparency upfront is not an appropriate accountability mechanism in this context.

**<u>Recommendation</u>: Acknowledge that, in line with the guidance on transparency, where a controller is carrying out research that cannot be based on consent (such as for fraud**

[16] See, House of Lords, Report on debate on Data Protection Bill, 11 December 2017, Volume 787, available https://hansard.parliament.uk/lords/2017-12-11/debates/154E7186-2803-46F1-BE15-36387D09B1C3/DataProtectionBill(HL).
[17] See footnote 16 at Column 1446.

**prevention purposes), or where the interface with the individual prevents extensive information provision, controllers can adopt a layered approach and provide more detailed information elsewhere (consistent with the fact that some information may not be provided in fraud-prevention and similar contexts).**

Also, on page 27, the WP states that "where purposes are unclear at the start of a scientific research programme, controllers will have difficulty to pursue the programme in compliance with the GDPR". This sentence should be reworded, as it seems inconsistent with the various helpful solutions offered by the WP on the following page that do describe a way forward on using personal data for research (such as anonymisation and providing more general information coupled with incremental specific consents for specific project phases as a research project progresses), even where all purposes are not sufficiently clear for obtaining specific consent up front. However, the solutions do not remove all potential problems concerning the ability to use personal data for research.

For example, on page 28 the WP states:

> Also, having a comprehensive research plan available for data subjects to take note of, before they consent could help to compensate a lack of purpose specification. This research plan should specify the research questions and working methods envisaged as clearly as possible. The research plan could also contribute to compliance with Article 7(1), as controllers need to show what information was available to data subjects at the time of consent in order to be able to demonstrate that consent is valid.

Providing a comprehensive research plan as a way to compensate for a lack of purpose specification goes beyond what is needed for consent. It is unlikely that disclosing scientific methodologies and questions would increase an individual's trust in a controller's data processing, but rather make the consent itself lengthy and unintelligible for an average research participant.

It will also have a negative impact on intellectual property rights and business confidentiality, resulting in the stifling of scientific innovation. Patents can and have been denied where comprehensive plans that include working methodologies have been disclosed to the public. For example, a currently pending case in the European Patent Office (EPO) involves a holding by the Technical Board of Appeal of the EPO that a patent is invalid for lack of inventive step in view of the detailed information that was contained in an informed consent form document used in a clinical trial.

**<u>Recommendation</u>: Clarify that making a "research plan" available to individuals does not entail disclosing scientific methodologies as such disclosures would carry significant risks for organisations' property and intellectual property rights, undermine innovation, as well as diminish actual transparency to individuals.**

On page 29, the WP states the following:

> It is important to remember that if consent is being used as the lawful basis for processing there must be a possibility for a data subject to withdraw that consent. WP29 notes that withdrawal of consent could undermine types [of] scientific

research that require data that can be linked to individuals, however the GDPR is clear that consent can be withdrawn and controllers must act upon this – there is no exemption to this requirement for scientific research. If a controller receives a withdrawal request, it should delete or anonymise the personal data straight away if it wishes to continue to use the data for the purposes of the research.

The withdrawal of consent should not jeopardize the scientific research. The position of the Guidance is too restrictive and would, for example, collide with the regulations on clinical trials, since the deletion of the data of a patient who exercises the right to withdraw consent would harm the clinical trial process and would also collide with the regulation on clinical trials that will enter into force in 2019.[18]

If a patient withdraws consent, the data already obtained should be available for the study at stake, without need to anonymize it and of course, without having to delete it. This is also the position taken by the Clinical Trials Regulation, as stated above.

**Recommendation: Clarify that a withdrawal of consent should not jeopardize scientific research through the deletion of data that has already been provided and that is part of the study.**

### C. Consent obtained under Directive 95/46/EC (p. 29)

The WP states on page 29 that if pre-existing consents are not in compliance with the GDPR, they must be re-obtained (with some limited exceptions, such as where some of the new notice elements were not given under the Directive). In other words, all post-25 May 2018 consents must "meet the GDPR standard." The WP's guidance on existing consents is more restrictive than necessary and impractical.

CIPL's May 2017 "Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR"[19] proposed that, generally, pre-GDPR consents should continue to be valid if they were obtained in compliance with the Directive and national law. Organisations should not have to re-paper existing consent until there is a material change in processing and its purposes. The only exception might be cases where existing consents do not comply with the GDPR's requirement that "utmost account shall be taken of whether, *inter alia,* performance of a contract, including provision of a service is conditional

[18] See also the FDA's 2008 Guidance for Sponsors, Clinical Investigators, and IRBs regarding "Data Retention When Subjects Withdraw from FDA-Regulated Clinical Trials" (https://www.fda.gov/downloads/RegulatoryInformation/Guidances/UCM126489.pdf): 1. FDA regulations require clinical investigators to maintain case histories of each individual who participates in a clinical trial, including information on subjects who withdraw from a clinical trial. According to FDA regulations, when a subject withdraws from a clinical study, the data collected on the subject up to the point of withdrawal needs to remain part of the study records and may not be removed. Deletion or anonymization of this data would conflict with guidance and regulations regarding clinical studies (such as the FDA). 2. Deletion or anonymization of this data could also undermine the scientific validity and ethical integrity of a clinical trial. Removal of data from a trial database could jeopardize the ability to access data on adverse events, which could have adverse impact on societal health, safety and wellbeing. Non-random removal of data from a clinical study could affect the scientific validity of clinical research, e.g. by distorting the effectiveness of the results or hiding important safety information.

[19] See footnote 2.

on consent to the processing of personal data that is not necessary for the performance of that contract" (see Article 7.4) or, in connection with a child, the requirements of Article 8(1) have not been met.[20]

Implementing the WP's guidance with respect to all existing pre-GDPR consents and processing activities would be a practical impossibility at this stage with no significant countervailing benefits for individuals. In fact, the individuals would be faced with the significant burden and potential annoyance of having to re-consent to activities to which they had previously consented and that have not changed.

**Recommendation: Amend the guidance to reflect the more narrow and pragmatic consent "updating" requirements suggested above whereby only those existing consents must be updated that (a) do not comply with the GDPR's requirement that, in determining "whether consent is freely given, utmost account shall be taken" of whether performance of a contract or service is conditioned on consent to processing that is not necessary for the performance of a contract or, (b) where, in connection with a child, the requirements of Article 8(1) have not been met, bearing in mind that companies must be able to, at a minimum, retain the personal data and contents with respect to users who as of 25 May 2018 will be deemed children under the age of digital consent so that the users can access that data or resume the service upon reaching the age of consent without losing the personal data and content they have stored in the service.**

### D. Impact of status change to sensitive data

Obtaining consent for ongoing processing where consent previously was not required will be difficult or impossible if the controller does not have access to user data, which is often the case. Indeed, this situation is particularly problematic in the context of children's data that as of 25 May will be subject to parental consent. While one generally could present a consent request to all existing users logging onto a service from 25 May onward, with respect to children, there is no way knowing for sure (without asking the user to self-assert) their country and age to determine if any children require parental consent under Article 8(1).

Also, companies may end up having existing users for whom the company has been providing services and lawfully processing personal data, perhaps for years, and who, as of May 25, are deemed children and whose parent now must give consent. That could put their personal data, including content and the actual service, in limbo until the parent gives consent. CIPL recommends that the WP confirm that companies will, at a minimum, be able to retain those users' personal data and content (unless the user requested deletion under

[20] In fact, this seems to be consistent with the September 2016 opinion of the German DPAs of the Duesseldorfer Kreis on this issue Beschluss der Aufsichtsbehoerden fuer den Datenschutz im nicht-oeffentlichen Bereich, (Duesseldorfer Kreis am 13./14. September 2016), Fortgeltung bisher erteilter Einwilligungen unter der Datenschutz Grundverordnung, available at https://www.lda.bayern.de/media/dk_einwilligung.pdf (providing that pre-existing consents in principle will meet the conditions of the GDPR and will, therefore, continue to be valid but special focus should be given to the "conditionality" provision under Article 7(4) GDPR and the children's age of consent issue under Article 5(1), the requirements of which may not be met by pre-existing consents.)

Article 17(1)), so that the users can access that data or resume the service upon reaching the age of digital consent, or upon receipt of parental consent, without losing the personal data and content they have stored in the service. The companies would, of course, need to respect the exercise of individual's rights throughout.[21]

**Recommendation**: **Confirm that, consistent with the GDPR requirements on erasure, companies may, at a minimum, retain the personal data and contents with respect to users who as of May 25 2018 will be deemed children under the age of digital consent so that the users can access that data or resume the service upon reaching the age of consent without losing the personal data and content they have stored in the service.**

## Conclusion

CIPL is grateful for the opportunity to provide further comments on key implementation questions regarding consent under the GDPR. We look forward to providing further input on consent in the future as new issues arise, particularly in light of practical experiences in applying the GDPR.

If you would like to discuss any of these comments or require additional information, please contact Bojana Bellamy, bbellamy@hunton.com, Markus Heyder, mheyder@hunton.com or Sam Grogan, sgrogan@hunton.com.

[21] As noted above, CIPL will present a fuller paper on the challenges in respect of children's data requirements in the GDPR. We make this one children's data point here to highlight the challenges in respect of existing users and existing processing prior to May 2018 to demonstrate practical compliance issues.