29 January 2018

Comments by the Centre for Information Policy Leadership

on the Article 29 Data Protection Working Party's

"Guidelines on Transparency"

adopted on 28 November 2017

On 28 November 2017, the Article 29 Data Protection Working Party ("WP") adopted its "Guidelines on Transparency 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 cases, the Guidelines elaborate usefully on the GDPR's transparency requirements. In particular, CIPL welcomes the following items:

- The emphasis on user-centric transparency and the discussion of how to reconcile such transparency with full legal disclosures, such as through the layered approach to providing information and the concept of "push" and "pull" notices.

- The statements on the use of visualization tools and, in particular, icons, and that any development of a code of icons should follow an "evidence-based approach", be preceded by research, and conducted "in conjunction with industry and the wider public as to the efficacy of icons."

- The recognition of the role of user testing of different modalities for providing information before "going live" or committing to a particular approach.

- The discussion of the multitude of modalities controllers may choose from to provide information to individuals, including transparency tools that provide "tailored information" to the user.

- The recognition of the importance of avoiding overly detailed technical or legalistic language.

- The emphasis on accessibility, inclusiveness and consideration of people with disabilities and other vulnerable populations when designing transparency measures.

[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.

CIPL has also identified several areas in the Guidelines that would benefit from further clarification or adjustment, as set forth in our comments below.

Comments

I. Comments on Introduction (p. 5)

By way of a general comment, the WP should more clearly acknowledge, in the Introduction, the underlying tension between asking for clear and concise notices that are "transparent, intelligible, and easily accessible" while still including all of the information required by the GDPR and/or recommended by the WP. Acknowledging this tension should be a continuing theme throughout the Guidelines and all recommendations should be considered in light of it. Indeed, CIPL takes the view that Articles 13 and 14 GDPR already require sufficient information. Requiring even more information does not seem to be in line with the goal of transparency.

Furthermore, the WP should acknowledge in the Introduction that the GDPR is grounded in a risk-based approach. Thus, rather than requiring a controller to automatically provide individuals with detailed analyses in every context, the GDPR demands that controllers proactively engage in detailed risk assessments to inform individuals about the most impactful types of data processing. It allows organisations the opportunity to decide what to prioritise in their transparency and information provided to individuals as well as to calibrate the depth and the level of detail of information based on the underlying risk of the processing. This approach would also be in line with the recognition in the Introduction (para. 2) that transparency is an expression of fairness and closely linked to the principle of accountability.

Recommendation: Acknowledge the tension between transparent, intelligible and easily accessible notices and providing comprehensive information. Acknowledge that the risk-based approach also applies to how to prioritise what information should be provided to individuals and to what level of detail.

II. Comments on "Elements of transparency under the GDPR" (p. 7)

A. Providing information about the risks of processing (p. 8)

On page 8 (para. 9), the WP states that "as a best practice, in particular for complex, technical or unexpected data processing, [ ] controllers should not only provide the prescribed information under Articles 13 or 14, but also separately spell out in unambiguous language what the most important consequences of the processing will be: in other words what kind of effect will the specific processing described in the privacy statement/notice have on a data subject." In addition, the WP states that this description of consequences should not be limited to "best case" examples but should "provide an overview of the types

of processing that could have the highest impact on the fundamental rights and freedoms of data subjects in relation to protection of their personal data."

While the WP does not define "consequences", the focus appears to be on the potential negative consequences of data processing. Expecting controllers to describe in detail ("spell out")[2] — and, more likely, in many cases to speculate on — the potential negative impacts of their processing is problematic for a number of reasons.

First, the GDPR does not list this kind of information in Articles 13 and 14, which in and of itself is meaningful. Had the drafters wanted to include this information, they could have done so. Second, the exact scope and nature of what would have to be disclosed on this point is so vague and subjective that it would be difficult to implement — much less evaluate for compliance purposes in any consistent manner. Third, it would place controllers in the untenable position of having to potentially undermine their own processing operations by publicly describing speculative risks and harms that may only generate unnecessary concern.

Providing this kind of disclosure goes beyond the GDPR's principle of transparency and is potentially inconsistent with the principle. Where appropriate and required under the GDPR, individuals should be made aware of the fact that any processing risks have been identified and appropriately safeguarded against (See Recital 39). However, as currently worded (and despite the WP calling this only a "best practice"), the Guidelines risk introducing an unbounded obligation or expectation for organisations to spell out potential negative impacts of their processing operations. Moreover, descriptions of potential hypothetical scenarios would swamp individuals with even more information, thereby impeding effective communication of relevant information and undermining transparency.

<u>Recommendation</u>: To avoid introducing a new disclosure obligation on organisations not found in the GDPR, qualify the scope of the recommended best practice of spelling out potential risks and harms associated with processing by clarifying that controllers must exercise their judgement in whether and how to provide effective and actionable transparency concerning the possible consequences of their processing, consistent with the GDPR.

B. "Easily Accessible" (p. 8)

In the example box on page 8 (para. 10), the WP states that in apps the necessary information "should never be more than 'two taps away'". The "two taps away" standard is too rigid and unnecessarily encroaches on app design as well as potentially interferes with user experience. It should be sufficient to require that the relevant information is clearly marked and easily accessible, which gives controllers some flexibility to ensure that they are providing the required accessibility in a way that takes into account user experience.

[2] See p. 8 of the Guidelines.

Recommendation: **Delete the "two taps away" reference to avoid unnecessary interference with app design and user experience.**

C. "Clear and plain language" (p. 9)

Discussing the issue of what it means to provide information in "clear and plain language", the WP states on page 9 (para. 12) that terms such as "may", "might", "some", "often" and "possible" should be avoided. Even though the WP does not suggest prohibiting these terms, it creates a presumption that these terms lack clarity. But they do not in many cases.

In many cases, these terms may more accurately reflect the state of available information than more definitive terms might. For example, stating that certain processing "will" occur when, in fact, it only "may" occur would be inaccurate and misleading. Often there are cases where processing is possible but not certain, such as sharing information with law enforcement. In short, the terms "may", "might", "some", "often" or "possible" may be the most accurate and appropriate terms available in a given circumstance.

For example, the term "may" would be the most accurate where, in connection with a compatible secondary use of personal data for scientific research, the personal data was initially collected for one purpose but the initial disclosures included a statement that it may or might (or not) be used for scientific research in the future, subject to required GDPR safeguards.

Another example of where such terms may be more accurate is where certain processing is dependent upon an individual's use of a service or of relevant controls. In such a case, the controller can only accurately say that certain processing may occur — e.g. data may be used for personalized ads but it may not if a user decides to use a control limiting personalized ads.[3]

Finally, and for the same reasons, the WP should reconsider its examples on page 9 (para. 11) of phrases that are not sufficiently clear because of the term "may." (E.g. "We *may* use your personal data for research purposes," or "We *may* use your personal data to offer personalized services").

[3] Indeed, in a few instances the guidance from the WP itself bears out the notion that terms like "may" can be appropriate. For example, on page 20 (para. 38) concerning "information related to a further processing" the WP's description illustrates the point that language qualifiers such as "may" are appropriate to use: "Where personal data are further processed for purposes that are compatible with the original purposes (Article 6.4 informs this issue), Articles 13.3 and 14.4 apply. The requirements in these articles to inform a data subject about further processing promotes the position in the GDPR that a data subject should reasonably expect that at the time and in the context of the collection of personal data that processing for a particular purpose may take place." (Emphasis added) Also, on page 28 (para. 58), the WP provides an example of where a data controller's provision of information to an individual under Article 14.1 may impair the achievement of the processing objectives. However, the WP explains that the account holders should at least have information about the fact that their personal data "may be processed" by the bank for anti-money laundering purposes.

<u>Recommendation</u>: Delete the statement that qualifiers such as "may", "might", "some", "often" and "possible" should be avoided and remove the examples in paragraph 11.

D. "the information may be provided orally" (p. 11)

On page 11 (para. 16), the WP notes that under Article 12.1, "information may be provided orally to a data subject on request, provided their identity information is proven by other (i.e., non-oral) means". The WP should clarify that this means that proof of identity cannot be based on oral statements to the effect of "I am so and so", but it does not mean that voice recognition cannot be used or that verbal identity-confirming questions and answers cannot be used. The methods used to verify identity should be neither foreclosed nor prescribed.

<u>Recommendation</u>: Delete in paragraph 16 the phrase "by other, i.e., non-oral means".

III. <u>Comments on Information to be provided to the data subject - Articles 13 & 14</u> (p. 12)

A. User testing for validating the effectiveness of transparency (p. 7 and p. 13)

The WP states that controllers looking to validate their approach to giving users adequate notice should do so through user panels or other similar user testing: "Controllers can demonstrate their compliance with the transparency principle by testing the intelligibility of the information and effectiveness of user interfaces/notices/policies etc. through user panels" (para. 8). Moreover, the WP suggests that such usability and readability studies can help controllers to validate their chosen approach, assisting them with meeting their "accountability obligations" (para. 21).

Although CIPL agrees that user panels can provide helpful feedback to controllers building their privacy notices, they are not the only means for validation. The WP should also highlight other possible testing mechanisms for validating compliance with the GDPR's transparency requirements, including through both formal and informal interactions and conversations with industry groups, consumer advocacy groups, and even regulatory bodies about a controller's proposed approach to a new or existing privacy notice. Indeed, user panels may be the right audience to evaluate the effectiveness of consumer-facing settings and privacy dashboards, but they are certainly not the best group to evaluate the overall "effectiveness" of a privacy statement. The WP appears to acknowledge that reality in its guidance, noting that most users "will only glance over communications of changes to privacy statements/notices" (at para. 22). And there are many studies that validate that view.[4]

[4] See, e.g., Omri Ben-Shahar & Adam S. Chilton, *Simplification of Privacy Disclosures: An Experimental Test* 1, 28 (University of Chicago Coase-Sandor Institute for Law & Economics Working Paper No., 737, 2015), http://ssrn.com/abstract=2711474 (describing results of experiments in which different simplified approaches to privacy statements had no significant impact on users' comprehension or choices).

<u>Recommendation</u>: The WP should explicitly recognise that there are other mechanisms than "user testing" to evaluate the transparency and effectiveness of a privacy statement. CIPL recommends including further examples of appropriate instruments in the Guidelines.

B. "Appropriate Measures" – template and model notices (p. 12 and p. 13)

On pages 12-13 (para. 20), the WP addresses the issue of privacy notices and privacy policies, noting that the GDPR does not prescribe the format or modality but leaves it to the controller to take appropriate measures based on a number of contextual factors. While this flexibility is essential, it might be helpful to provide specific examples of effective and not so effective notices. The examples provided by the UK Information Commissioner's Office could be helpful in this respect.[5]

<u>Recommendation</u>: Consider including in the guidance examples of appropriate measures, such as the ones provided by the UK Information Commissioner's Office at https://ico.org.uk/media/for-organisations/documents/1625136/good-and-bad-examples-of-privacy-notices.pdf.

C. "Appropriate measures" – notifying changes to privacy policy (p. 13)

On page 13 (para. 22), the WP notes that accountability with respect to transparency applies not only at the point of collection but "throughout the processing life cycle" including when "changing the content/conditions of existing privacy statement/notices." Thus, the WP suggests that "any" changes must be notified to the individual affirmatively.

While it makes sense to require an organisation to individually communicate changes that are "indicative of a fundamental change to the nature of the processing" (para. 26) or other significant updates that materially impact the data subject, the GDPR should not be read to require such communications for every kind of change. Changes that generally should not have to be notified include:

- corrections to misspellings;
- updates to a mailing address or to hyperlinks;
- fixing stylistic or grammatical flaws to improve readability;
- rewording text in privacy notices based on customer feedback;
- updates to comply with GDPR requirements where the underlying processing does not change and the change only adds further detail;
- appointment of a new category of data processor;
- information about products and services covered in the privacy policy but not relevant to the particular individual;
- adding third-party analytics companies that have no bearing on the individual;
- describing a new cookie on a website targeted only to U.S. persons.

[5] https://ico.org.uk/media/for-organisations/documents/1625136/good-and-bad-examples-of-privacy-notices.pdf.

The above changes should not have to be notified unless the change is likely to have a significant impact on individuals. Instead, the organisation should be permitted to make those changes in the online privacy statement or notice and update the date on which the text was last revised. Requiring direct communications of immaterial changes may result in too frequent and unnecessary communications that are burdensome both to the organisation and to individuals, particularly in light of the fact that individuals would be receiving such updates from many controllers. Moreover, it is not unreasonable to acknowledge that individuals should have some ongoing responsibility by asking them to proactively look at privacy policies.

Indeed, this may be an appropriate place to make use of the "pull" model, as discussed in CIPL's May 2017 white paper on transparency, consent and legitimate interest under the GDPR.[6] To the extent the overarching goal is transparency as opposed to information overload, a "pull" approach would seem to better accomplish that aim. The WP acknowledges the utility of the pull approach for some purposes (see page 17, para. 32) and should consider expanding its application to this context.

Recommendation: Clarify in paragraphs 22 and 26 that organisations should send notifications of changes to privacy statements/notices to individuals where the changes are "fundamental" or "material", but may rely on individuals to find (or "pull") other updates online.

D. Timing of notification of changes to Article 13 and 14 information (p. 14)

On page 16 (para. 28), the WP adds that when data processing occurs on an ongoing basis, "the controller should reacquaint data subjects with the scope of the data processing" with reminders of the privacy statement at appropriate intervals, "even when transparency information (e.g. contained in a privacy statement/notice) does not materially change". CIPL believes that this practice will cause information overload for individuals and unnecessary administrative burden for organisations while at the same time failing to enhance privacy protections.

Some individuals subscribe to dozens if not hundreds of websites, apps and other services, each with its own privacy policy/notice. They may feel overwhelmed and annoyed by periodic "reminders" of these privacy policies/notices inundating their email inboxes, post boxes and other channels. Individuals should at least have the possibility to opt-out from receiving these communications.

CIPL believes that the WP has gone too far in absolving the individual of any responsibility to access available information even in low-impact contexts where no changes have been made. For the same reasons described in the point above (regarding the notification of

[6] CIPL "Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR", 19 May 2017, at p. 6-7, 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.

insignificant substantive changes), the WP should allow for more leeway and discretion on the part of organisations to decide when and in what intervals it is appropriate, useful and not burdensome and intrusive to individuals to send them reminder information or whether to make such information available through the "pull" model.

Recommendation: Either delete paragraph 28 or clarify that whether and in what intervals "reminder notices" should be sent to individuals, even when there have been no material changes to the privacy statement/notice, should be left to the judgment of the organisation. A decision on that point should be based on the organisation's assessment of whether such reminders would be useful and not burdensome or intrusive to the individual. Furthermore, where no changes to a privacy policy/notice have occurred, organisations should also be able to rely on the ability of individuals to find such policies/notices in an appropriately identified location online.

E. Modalities – format of information provision (p. 16)

On page 16 (para. 29), the WP states that "[t]he data subject must not have to take active steps to seek the information covered by these articles [13 and 14] or find it amongst other information." Taking into account the fact that the Guidelines suggest that links may be inserted to access notices as a valid mechanism, links should be expressly excluded from being considered an "active step" under paragraph 29.

Recommendation: Make it explicit that links to access notices are a valid modality for providing information and are not considered an "active step" under paragraph 29 of the Guidelines.

F. Layered privacy statements/notices (p. 17)

On page 17 (para. 31), the WP states that "aside from providing an online layered privacy statement/notice, data controllers may also chose to use additional transparency tools [...]" (Emphasis added). The use of the word "additional" confuses the sentence as the sentence presumably intends to convey that transparency tools other than online layered privacy notices may be used (as opposed to saying that such other tools must be "in addition" to layered notices and cannot be used alone).

Recommendation: Substitute "other" for "additional".

G. Information on profiling and automated decision-making (p. 19)

On page 19 (para. 34), the WP refers to its earlier guidelines on automated individual decision-making and profiling for its guidance on how to provide meaningful information on the "logic involved" in automated decisions. CIPL has provided comments on this particular guidance from the WP and addressed the issue of providing meaningful information on the

"logic involved" in its comments.[7] It recalls these comments here and recommends the WP to take them into account in the context of its guidance on automated decisions making and in its guidance on transparency.

Recommendation: Take CIPL's recommendations on the proper interpretation of meaningful information on the "logic involved" into account.

IV. Comments on Information related to further processing (p. 20)

A. Information on "compatibility analysis" (p. 21)

On page 21 (para. 40), the WP states in connection with processing for compatible purposes that "in adherence to the principle of transparency expressed in Article 12 and the essential requisites of accountability and fairness under the GDPR", organisations should provide individuals with "further information on the compatibility analysis carried out under Article 6.4" The WP does not define the scope of such "further information on the compatibility analysis", i.e. whether this means some or all of the compatibility analysis or a summary thereof.

Regardless of the intended scope, the GDPR does not require this type of additional information to supplement the GDPR's required disclosures. Articles 13.3 and 14.4 require only that the organisation provide the individual "information on that other purpose" and "further information as referred to in paragraph 2", and that does not include information about the compatibility analysis. The additional recommendation from the WP would undermine effective transparency in general by requiring the delivery of detailed information to individuals that would provide little corresponding benefits to their understanding of an organisation's data processing. Moreover, in doing so, the WP's recommendation would impose significant burdens on organisations forced to reformat, redact (because of the likely commercially confidential content of such analyses), compose and/or deliver such additional information regardless of the risks involved with the underlying processing.

The motivation to add additional disclosures in the name of transparency is understandable. However, as discussed in CIPL's earlier recommendations on this topic[8], transparency cannot be absolute. There is a marked tension between providing complete information about all relevant issues on the one hand and clarity on the other. Thus, transparency requires informational discipline on the part of organisations, especially in the context of the complexities of the modern digital economy. All GDPR information and disclosure

[7] Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Automated Individual Decision-Making and Profiling", 1 December 2017, at p. 16-17, available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_to_wp29_guidelines_on_automated_individual_decision-making_and_profiling.pdf.

[8] See footnote 6, CIPL "Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR" at pages 6 and 9.

requirements should be applied with that in mind in order to achieve the overarching goals of the GDPR.

Recommendation: Delete paragraph 40.

V. Comments on Exercise of data subjects rights (p. 23)

A. Modalities for facilitating the exercise of rights (p. 23)

On pages 23-24 (para. 48), the WP addresses the appropriate modalities for facilitating the exercise of individuals' rights under the GDPR. On page 24, it provides a "Good Practice Example" and a "Poor Practice Example." As to the "poor practice" example, having dedicated contact points for rights requests, often an e-mail address monitored by more than one person, is common, user-friendly and reasonable and has proven to be effective in practice.

Recommendation: Clarify that the "Poor Practice Example" is only poor if the statement on the website does not contain the relevant contact information for customer services.

VI. Comments on Exceptions to the obligation to provide information (p. 24)

A. Article 13 exceptions (p. 24 and p. 25)

On page 25 (para 49), the WP states in its "Example" regarding Article 13 exceptions that an individual must be provided with new information under Article 13 whenever there is a new purpose of processing (here a messaging service) and that, as a "matter of best practice," all the information under the notice requirement should be provided again, even if individuals received that information before. The approach in the Example directly contradicts Article 13.4, which provides that Paragraphs 1, 2 and 3 of Article 13 shall not apply "insofar as the data subject already has the information." For that reason, the WP should delete the example. Alternatively, it should clarify that there may be circumstances where it would be helpful to provide individuals with all of the information again, but organisations may choose to do so at their discretion. That said, even with a revised version of the example, the WP should explicitly acknowledge that providing such information again could distract individuals from focusing on any new key information regarding data processing, serving to undermine transparency rather than advancing it. This context may also be an appropriate application for the "pull" model discussed on page 17 of the Guidelines.

Recommendation: To bring the Guidelines in line with Article 13.4, remove the statement/example to the effect that controllers should re-provide as a matter of best practice old information when providing new information in connection with a new purpose. Clarify that providing such old information should be left within the discretion of the controller if it finds that this would be useful and not undermine overall transparency.

B. "Impossible" or "Disproportionate effort" (p. 27 and p. 28)

On page 27 (para. 55) the WP limits the use of Article 14.5(b) on "disproportionate efforts" beyond what is required by the GDPR. This limitation could seriously harm the public interest and lead to information overload of notices to individuals pursuant to Article 14. The WP concludes that "the exception cannot be routinely relied upon by data controllers who are not processing personal data for the purposes of archiving in the public interest, for scientific or historical research purposes or statistical purposes".

That conclusion inappropriately takes the "examples" from GDPR Recital 62 and makes them the only contexts in which an organisation can routinely limit the provision of information because this requires disproportionate efforts. On the contrary, Article 14.5(b) also recognises that information to individuals may be restricted if it would seriously impair the objective of processing, for example in connection with the use of collected data for lawful purposes such as confirming identity or prevention of fraud, terrorism, and money-laundering, or for economic sanctions and export control compliance. Many services used for these purposes on a legitimate interest legal basis involve data indirectly obtained about individuals that have nothing to do with archiving for research or similar purposes. Yet any interpretation of Article 14.5(b) to require that notices are sent to every single individual having data in such services would either render these critical services too expensive to be used, overwhelm individuals with notices, or alert "bad actors" by omission that they are not on a watch list and may proceed with criminal plans. Finally, the reference and example of serious impairment of objective in Art 14.5(b) is just an example of where the provision of information to individuals proves impossible.

Recommendation: Delete the conclusion that the disproportionate efforts clause cannot be routinely relied upon by data controllers who are not processing personal data for the purposes of archiving in the public interest, for scientific or historical research purposes or statistical purposes.

On page 28 (para. 57), the WP states that where a data controller

> seeks to rely on the exception in Article 14.5(b) on the basis that provision of the information would provide a disproportionate effort, it should carry out a balancing exercise to assess the effort for the data controller to provide the information to the data subject against the impact and effects on the data subject if he or she was not provided with the information.

However, the GDPR does not require this kind of risk assessment or balancing test. The "disproportionality" at issue in Article 14.5(b) expressly refers to the disproportionality between the effort associated with "provision of such information" and the intended data use. It does not refer to any disproportionality between the controller's efforts to provide the information and the impact on the individual if he or she did not have such information. Accordingly, the WP should remove the recommendation that controllers engage in a balancing test between these two items.

This is not to say, of course, that the controller should not engage in a risk assessment and balancing of rights and interests on the underlying processing activity — indeed, the GDPR demands it. Under Article 14.5(b), the controller must "take appropriate measures to protect the data subject's rights and freedoms and legitimate interests."

Recommendation: Remove the reference, in paragraph 57, to a balancing exercise between the effort involved in providing information to the individual against the impact of not providing the information to the individual.

VII. Comments on the Schedule — Information that must be provided under Articles 13 or 14 (p. 31)

In the Table on page 31, the WP states in the box on the identity and contact details of the controller, that the information provided should ". . . preferably allow for different forms of communications with the data controller (e.g. phone number, email, postal address etc.)".

We recommend that the WP state that where contact details of the data protection officer have been provided according to Article 13.1(b) and Article 14.1(b) it would normally be sufficient to limit the information about the controller (or the controller's representative where applicable) to providing the identity only, since the individual will already have the necessary contact detail information of the data protection officer in order to address any of his or her rights. (Moreover, the controllers contact details will always be on its website). Indeed, having dual contact details will lead to information overload and is contrary to keeping notices concise and simple. This is also consistent with Article 38.4 which states that data subjects may contact the data protection officer with regard to all issues related to processing of their personal data. However, in the event the controller has not appointed a data protection officer it, of course, makes sense to include the contact details for the controller.

Recommendation: Clarify that where the contact details of a data protection officer have been provided the contact details of the controller do not need to be provided.

In the Table on page 31, the WP states in the box on legitimate interests as the legal basis that "[a]s a matter of best practice, the data controller should also provide the data subject with the information from the balancing test. . .".

The GDPR does not require controllers to hand over this information to individuals. While a data subject is entitled to receive information about the legitimate interests pursued by the controller, that information does not include actual documentation of, or any further information about, the legitimate interest balancing test the controller performed.

Moreover, it is worth noting that such balancing tests are confidential business information that may contain trade secrets and other important details about a controller's data processing systems that are typically not disclosed to third parties.

Finally, where a controller relies on legitimate interest for multiple processing purposes, information on the underlying balancing tests for each of these could add significant amounts of information to the already extensive mandatory information disclosures under the GDPR.

Recommendation: Remove the suggestion that controllers should, as a matter of best practice, disclose to individuals the details and outcome of the balancing test underlying the controller's decision to rely on the legitimate interest ground for processing.

On page 32, in the box on "recipients or categories of recipients" the WP interprets Articles 13.1(e) and 14.1(e), both of which require controllers to disclose to individuals "the recipients or categories of recipients of the personal data." Even though the GDPR clearly states "recipients or categories of recipients" in the alternative without privileging one or the other, the WP asserts that "[i]n accordance with the principle of fairness, the default position is that a data controller should provide information on the actual (named) recipients of the personal data." According to the WP, if the controller chooses the option of providing "categories of recipients" it must be able to demonstrate why this is fair. In addition, the WP suggests that controllers must identify industry, sector, sub-sector and location for these recipients.

The WP's interpretation of these provisions demands more than the plain text of the law requires. Moreover, the value of this information for the individual is questionable and the notion that more information in this context is better goes against the underlying principle of transparency.

Recommendation: Amend the WP's interpretation to reflect two co-equal options of disclosing "recipients" or "categories of recipients," and remove the references to fairness and to the specifications of categories of recipients.

On page 33, in the box on "transfers to third countries", the WP says that the information "should explicitly mention all third countries to which the data will be transferred." According to Articles 13.1(f) and 14.1(f), the GDPR only requires information "that" such transfers are intended and information about the existence or absence of an adequacy decision, and, in some cases, information on the appropriate or suitable safeguards in place. The GDPR has no requirement to identify the names of "all third countries." Indeed, such an obligation would unnecessarily increase the complexity and density of the information provided under this paragraph by orders of magnitude, particularly since any such interpretation would leave unclear whether "transferred" includes "accessed" from a third country.

Recommendation: Delete the statement that controllers should explicitly mention all third countries to which personal data will be transferred.

On page 35, in the box on "source from which the personal data originate", the WP adds requirements not found in the GDPR, all of which should be deleted. While Article 14.2(f) only requires provision of information on "from which source the personal data originate,

and if applicable, whether it came from publicly accessible sources," the WP adds that the information should also include information on "the nature of the sources" such as "types of organisations/industry sector" and "where the information was held (EU or non-EU)". Again, this goes well beyond what the GDPR requires, adding unnecessary volume and complexity to the GDPR's already complicated transparency requirements without benefit to the individual. Instead, the information overload that individuals would face under this interpretation would effectively undermine transparency.

Recommendation: Delete the guidance demanding source disclosures that are not found in Article 14.2(f).

Conclusion

CIPL is grateful for the opportunity to provide further comments on key implementation questions regarding transparency under the GDPR. We look forward to providing further input on transparency 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.