Consultation on Transparency and International Data Transfers under the GDPR

Irish Data Protection Commissioner

13 October 2017

TRANSPARENCY UNDER THE GDPR

1. **There is no definition of transparency under the GDPR, although Recitals 39 and 58, amongst others, are informative as interpretative guides. How should transparency be defined/ interpreted?**

- Transparency is a central concern for companies as it directly relates to the trust that users put in them and in online services in particular. To be meaningful, transparency goes beyond a mere legal compliance exercise and, to truly benefit customers, it should be centred around their real needs. The achievement of truly effective and meaningful transparency for customers is a core impetus for companies, yielding significant benefits beyond merely safeguarding compliance.

- Recitals 39 and 58 of the GDPR contain important elements regarding the interpretation of transparency. The information provided to data subjects should be **"easy to understand",** written with **"clear and plain language"**, in a **"concise"** way and it should be **"easily accessible"**. The GDPR also recognises the importance of visualisation to make the information easy to understand. These elements clearly indicate that transparency should be designed with the objective of providing meaningful information to data subjects in a user-centric concise format rather than lengthy and technical information that would not be easily understood.

- "**Easy to understand"** and **"clear and plain language"**: over the years, data processing has become more complex in technical terms. This technological complexity can be a barrier for a non-specialist to fully understand how data is being processed, although the fundamental principles of what data is processed and why often remains straightforward. In this context, it is crucial that transparency is adapted to individuals who do not have a technological background and/or knowledge and that the information provided can be easily understood and digested by the average user. However, this accessible information should be supplemented by more detailed technical information which is available to those who are willing or able (regulators, media, privacy advocates etc.) to examine that information to assess the security and privacy promises made by data controllers. The balance between exhaustiveness and clarity should always be resolved in favour of clarity for customers at the point of data collection.

- **"Concise":** concise information is key to providing meaningful information to customers. We know that individuals only dedicate a small amount of time to consuming information notices before using a service online. We should accept that this situation is not going to change and instead of overloading the user with information that we know will further confuse and perhaps make them more likely to just tick a box, regulators should instead focus on methods designed to engage the user with relevant just-in-time information. Companies equally need to take this important constraint into account to ensure that the information provided safeguards real transparency. By specifying that information should be concise, the GDPR recognises that companies have flexibility in the level of details that should be provided, and that to be meaningful to customers, information should focus on the core important and non-obvious aspects of the data processing, rather than an exhaustive and technical description of the processing.

- **"Easily accessible":** To be effective, information should be easily accessible. This can be achieved by several means. Data controllers are best placed to determine where to provide the relevant information to ensure that it is accessible when needed. Online service users are accustomed to accessing links to core privacy documents in certain areas on websites and within certain menus / areas most relevant to the data collection.

- **Visualisation** will play an important role in the way the information will be understood by users. A layered approach can, for example, cater to users of all levels of technical knowledge and personal interests; ensuring that all are provided with the core essential information about what and how their data is processed, in a short, engaging and potentially pictorial form, with more detailed and fulsome information available for those users who wish to understand in more detail the practices of the data controller. Genuine efforts to achieve engagement from data subjects in the presentation of information should be viewed positively by regulators when assessing transparency efforts. There is a concern that regulators will seek to maintain traditional approaches in seeking the provision of detailed information to all data subjects, while also taking issue with the length of such documents.

2. **Article 12.1 of the GDPR requires a data controller to take "appropriate measures" to provide the information required under Articles 13 and 14 and any communications under Articles 15 – 22 and 34 relating to processing, in accordance with the transparency requirements set out in that Article. In other words, the information/ communication in**

question should be concise, transparent, intelligible, easily accessible and use clear and plain language.

a) What factors should be taken into consideration when determining what may be "appropriate measures" for these purposes?

- The best way for data controllers to be transparent about how they use data is to provide that information when and where it is most meaningful to their users. Companies are in the best position to determine this because they understand the needs of their users, and how people engage with their services.
- Regulators should ask whether people have the information they need to make informed choices about their data — not whether that information was delivered according to a specifically defined format.
- At its core, this means that user experience should be at the centre of how transparency is being designed by companies.

b) What sorts of transparency tools/ techniques/ mechanisms/ approaches might constitute "appropriate measures" for these purposes?

- A layered approach to transparency enables users to access more detailed information about their data if they wish.
- Transparency tools should accommodate innovation, adapting to evolving uses of data.
- Data subjects want to have access to information in a variety of formats. Expectations around transparency need to be flexible and technology-neutral in order to account for the new types of interfaces that will emerge in the future.
- It should also be acknowledged that information can be provided in different ways, whether it is in written form, oral explanations, videos, tutorials, or visualisations.
- Appropriate measures can include:
    - Privacy Policy
    - Privacy or control centres (and other dashboards) where users can review their activity on the service
    - Visualisations
    - Help centre pages and FAQs in a user-friendly format
    - Education pages providing information on how products function
    - In-product information: pop-ups, fly-outs, interstitials

- Chatbots
- Human interface
- Detailed technical working papers in support of more readily accessible information

3. **Recital 58 and Article 12.1 of the GDPR in particular indicate that there should be a higher transparency threshold when the data subject is a child. How should the higher level of transparency that is required when addressing child data subjects be achieved?**

- Millions of teenagers are already online and access online services every single day. We know that teenagers are already some of the most safety and privacy savvy online users. Recent surveys show that teens are very knowledgeable about how to control the information they share online.[1]

- Companies need to provide transparency for a general audience, across a range of ages, various reading abilities and various levels of familiarity with technology. For this reason, as a rule, companies should provide clear information that can be understood by all individuals. Companies will therefore be mindful of this and will aim to design transparency tools to be understood by all users.

- Companies that are not aware whether their services are being used by children, might not be in a position to target specific information. On the other hand, companies that are aware of this, should be encouraged to create dedicated spaces to help educate children and parents on privacy and safety. Data Protection Authorities (DPAs) can play an important role in encouraging this type of approach.

- Where specific spaces are created for children, special effort should be given to the language used. Appropriate and child-friendly design can also be a very efficient way to facilitate understanding by children.

4. **Article 12.1 also states that the information which must be provided to data subjects, as referred to in that article, should be provided "in writing, or by other means, including, where appropriate, by electronic means".**

[1] Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan. M, Smith, A. And Beaton, (2013) Teens, Social Media, and Privacy. *Pew Research Center* [online]. Available at: http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/ (accessed 10 October 2017).

a) What factors are relevant in determining whether the information might be provided in writing, or alternatively by other means, or by a combination of both?

b) What tools/ techniques/ mechanisms/ approaches might constitute "by other means", in a non-electronic environment, for these purposes?

c) What tools/ techniques/ mechanisms/ approaches might constitute "by other means", in an electronic environment, for these purposes?

- In an electronic environment "by other means" can include a large number of different ways to provide information. This could potentially include technologies that do not yet exist.
- Technology is evolving fast and although screens are the main interface today, this is likely to evolve quickly in the coming years. For example, in the near future it is possible that screens will be replaced, in some instances, by audio and virtual reality. The way to provide transparency will need to adapt to these new interfaces.
- For these reasons, the medium through which information is provided should not be strictly imposed and should remain technology neutral. The important point being that information is appropriately provided to individuals.

5. Article 12.7 provides that the information which is to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons. Article 12.8 provides that the European Commission is empowered to adopt delegated acts under Article 92 for the purposes of standardising the use of icons. What categories of information, to be presented by the use of icons, should be prioritised for the standardisation of icons?

- Icons are not a legal obligation and should not be imposed on companies. Icons are not always relevant for all types of services. Moreover, there is still a need for concrete evidence that icons can be beneficial to individuals — to date there is no consensus on this. Standardised icons also assume that all data controllers are collecting similar information. They do not and it would be deeply confusing for users to have to consume standard icons that are not applicable. There is also no clear solution to conveying information to users where no specific data is collected.
- The European Commission is empowered to adopt delegated acts to specify the use of icons. Industry should be consulted as part of this process to ensure that their experience and concerns are fully considered.

- In general, there should not be a standardised approach to icons as every company will have different needs and different ways to use them. Companies should have the liberty to use their own design that would adapt to their interface.

6. Article 13 sets out the information which must be provided to a data subject where personal data "are collected from the data subject" while Article 14 sets out the information which must be provided to a data subject "where personal data have not been obtained from the data subject". Which of Article 13 or 14 should apply (and why) where:

a) Personal data is collected remotely/ passively from a data subject i.e. it is collected from, or on, the data subject but without the data subject actively providing it to the data controller e.g. it has been collected by way of observation, CCTV recording, bluetooth "beacons" or wifi tracking of the data subject?

- Data collected remotely/passively from a data subject should be covered by Article 13 of the GDPR.

- The reference to wifi tracking and bluetooth beacons is considered potentially confusing as these means of collection should be configured to be anonymous wherever possible in which case no transparency obligations would arise under the GDPR.

b) Further personal data is inferred, derived or generated by a data controller from a set of personal data which was originally provided directly by a data subject to a data controller?

- The situation outlined appears to relate to a further use of personal data. The specifics determine whether it constitutes a use which requires reliance upon an additional legal basis in the GDPR. However, where data is directly collected from a user, Article 13 clearly applies regardless of any future uses.
- On the other hand, if the inferred data is provided by a third party, Article 14 of the GDPR should thus apply.

7. Article 13.3 and 14.4 both cover a situation where a data controller intends to further process the personal data for a purpose other than that for which it was collected/ obtained respectively. In such a situation, the data controller is required to provide the data subject with information on that other purpose "prior to that further processing".

a) How far in advance of that further processing should this information be provided?

- The timeframe between the provision of the information and the commencement of the further processing should be determined in order to be meaningful for individuals. If the

information is provided too early, the individual might forget. On the other hand, if individuals are not provided with sufficient time, they may not make the best decision.

- There should not be any strictly defined period of time before which information on further processing should be provided. The timing of the provision of information will be highly dependent on the context and it will vary from one situation to another.

- Companies are in the best position to know when it is best to provide this information to their users in order for it to be as meaningful as possible.

- When the further processing purposes are incompatible with the original ones, a new legal basis will be necessary.

b) What factors should affect the determination of the timeframe between the provision of this information and the commencement of the further processing?

- The level of unexpectedness can be one element to take into consideration to determine the appropriate timeframe between the provision of the information and the commencement of the further processing.

    - The more unexpected the further processing, the more in advance information should be provided to individuals.
    - On the other hand, if the further processing concerns "normal processing", which can be reasonably expected by individuals, e.g. processing to ensure the safety or security of a platform, or if the processing does not present any additional data protection/privacy implication the expectation is that this would be covered by information already available to users at the time of collection.

8. Recital 39 refers to the provision of certain information which is not explicitly covered by Articles 13 and 14 of the GDPR and specifically that "natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data.." What information (other than that set out in Articles 13 and 14) should be provided by data controllers to data subjects in connection with the "risks, rules, safeguards and rights"?

- Recital 39 does not intend to provide additional legal requirements to the right to information. In fact, articles 12 to 14 of the GDPR already appropriately cover transparency regarding "risks, rules, safeguards and rights in relation to the processing of personal data".

- The appropriate reading of Recital 39 is that a data controller is intended to outline all relevant information relating to data processing so that a data subject is in a position to

assess risks as determined by them. There is no expectation that a data controller will specifically seek to quantify risk.

9. The exceptions to the information requirements under Article 14.1, 14.2 and 14.4 are set out in Article 14.5. These include: where "the provision of such information proves impossible or would involve a disproportionate effort…"(Article 14.5(b)); and where obtaining or disclosure of the personal data is expressly laid down by EU or national law to which the data controller is subject and which provides appropriate measures to protect the data subject's legitimate interests (Article 14.5(c)).

- Transparency is not an absolute concept. Although it is a core data protection principle, it can be subject to limitations. The GDPR recognises that in some cases, providing information to a user is impossible or would involve disproportionate effort. Such an exemption would obviously not apply in the normal course where data is collected directly from data subjects.

- In cases where it is not, disproportionate effort would apply where the cost and time in contacting individual data subjects would outweigh the benefits that could arise from data processing. Disproportionate effort could also apply in relation to efforts to re-identify data in order to definitively identify an individual so as to make contact with them. The very act of doing this would undermine privacy protections.

a) How should the concept of "impossibility" be interpreted in accordance with Article 14.5(b)?

- This would apply where there are no verified contact details with which to make contact with an individual.

b) What should constitute a "disproportionate effort" in accordance with Article 14.5(b)?

- This would apply where there are no verified contact details with which to make contact with an individual.

c) Should the reference to the EU or national law referred to in Article 14.5(c) be interpreted as meaning that (i) the law requires the data controller to obtain or disclose the personal data on a mandatory basis or (ii) the law allows for - but does not make obligatory - the obtaining or disclosure of personal data?

- Article 14.5(c) should be interpreted as meaning that European Union or national law can derogate from Article 14 of the GDPR by adding situations where providing transparency to a data subject, where the data has not been collected from the data subject, should not

be mandatory, to the extent that appropriate measures to protect the data subject's legitimate interests are in place (interpretation ii).

d) What should constitute "appropriate measures to protect the data subject's legitimate interests" in the EU or national law referred to in Article 14.5(c)?

- "Appropriate measures to protect the data subject's legitimate interests" referred to in Article 14.5(c) of the GDPR could include:

  - Information should be kept for no longer than necessary;
  - Information should be kept in a secured way;
  - Appropriate confidentiality of the data should be ensured;
  - Data should be kept in a way to avoid any unauthorised access
  - Reasonable steps should be taken to ensure that personal data which is inaccurate is rectified or deleted.

10. How can information "fatigue" (which would undermine the positive benefits of transparency for the data subject) be avoided by data controllers while still ensuring compliance with all of the transparency requirements in the GDPR?

- It is widely recognised that exposing an individual to a great amount of information in a limited amount of time is not an effective way to provide transparency. Individuals, even when technology savvy, need to receive information in a way that they can comprehend and understand. When exposed to too much information, individuals are less likely:

  1) to fully understand the information
  2) to care about the information

- In order to avoid information fatigue, data controllers should be expected to focus on providing information at the right time, which may mean that the information will not be provided at once but at different moments in time (subscription, in product...) and that individuals have the possibility to go back to this information when needed (for example in a transparency/control centre).

- Adopting a layered approach to transparency will also enable users to digest the information at their own pace without drowning them in too much information which would undermine their understanding of the way data is processed.

TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS UNDER THE GDPR

1. **Which legal bases/ mechanisms for conducting personal data transfers to third countries or international organisations under the GDPR are likely to be most commonly relied on by your organisation?**

- While the Privacy Shield, Standard Contractual Clauses and consent are likely to be the most commonly used transfer mechanisms, companies shall use different transfer mechanisms for different activities.

- Companies will need the flexibility to rely on any of the available transfer mechanisms.

2. **What are the challenges to conducting personal data transfers to third countries or international organisations under each of the available legal bases / mechanisms set out in the GDPR?**

- The main challenge for companies is the legal uncertainty surrounding transfer mechanisms at the present time.

- The practical implications of changes to the available transfer mechanisms need to be considered as decisions are being made. Industry should be given adequate notice to adapt to any changes made to these transfer mechanisms.

3. **What specific actions might the Article 29 Working Party and / or national data protection authorities take to help organisations address or alleviate such challenges?**

- Companies seek certainty and consistency. It is essential that Article 29 Working Party ensures legal certainty for transfer tools. For example, following the annual review, the Article 29 Working Party should clearly express its support for the Privacy Shield mechanism. Support for the Privacy Shield mechanism has already been expressed by U.S. authorities and the European Commission in a joint statement following the annual review: "*The United States and the European Union share an interest in the Framework's success and remain committed to continued collaboration to ensure it functions as intended*".[2]

[2] European Commission (2017) Joint Press Statement from US Secretary of Commerce Ross and Commissioner Jourová on the EU-U.S. Privacy Shield Review[online]. Available at: http://europa.eu/rapid/press-release_STATEMENT-17-3342_en.htm

4. **What aspects of international personal data transfers under the GDPR should be prioritised for the purposes of guidelines which may be produced by the Article 29 Working Party and/ or national data protection authorities?**

- The Article 29 Working Party should focus on the new tools for transferring data provided by the GDPR: codes of conduct and certification. The Article 29 Working Party should work closely with industry to develop tailored and practical transfer mechanisms.

5. **If there are other aspects of international personal data transfers under the GDPR on which you have specific comments, proposals or questions (whether legal, practical, interpretative or otherwise), please provide us with this feedback.**

- Data transfer mechanisms should be treated equally by DPAs.

- DPAs should ensure that contractual transfer mechanisms are afforded a certain flexibility in interpretation, to take into account the existing business-to-business contractual arrangements in place between and within companies.
- Industry should be given adequate notice to adapt to any changes to the available data transfer mechanisms.

- Practical guidance should be provided for the situation where a head office located outside the European Union enters into data processing agreements with processors that will include the processing of personal data of its European affiliates. In practice the head office will negotiate the agreement on behalf of its affiliates. It is practically impossible to require all affiliates to sign these agreements as co-controllers.

- It would be useful to have an Article 29 Working Party non-binding template for a for a new vendor's security assessment that will process personal data.