EDPS response to the Commission public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy

On 24 September 2015, the European Commission launched a public consultation on online platforms (and, separately, on geo-blocking), as a part of its Digital Single Market strategy.

The range of questions in the consultation is quite broad and suggests a rather comprehensive approach of the Commission to the issues raised by online platforms. In particular, the consultation covers the social and economic role of online platforms; transparency (*e.g.* in search results); terms of use; ratings and reviews; the use of information by platforms; the relation between platforms and their suppliers; the conditions of switching between comparable services offered by platforms; the role of online intermediaries including ways to tackle illegal content on the Internet.

The EDPS, as an advisor to EU Institutions in the field of privacy and data protection, has long been concerned with the uncontrolled use of personal data to fuel the functioning of business models operated by (or linked to) online platforms (*e.g.* the EDPS Opinion "*Meeting the Challenges of Big Data*", referred to in footnote 5).

It is our aim, therefore, to contribute to this public consultation by limiting comments to areas of the consultation that have relevance for, or an impact on, the rights to privacy and data protection. To do so, we have reviewed the questions and selected those we considered to be most relevant for the individuals' rights to privacy and data protection which are protected under Articles 7 and 8 of the Charter of Fundamental Rights of the EU, Article 16 of the Treaty on the Functioning of the EU and in Directive 95/46/EC (the "Data Protection Directive").

Preliminary remarks

In general terms, we are concerned that the formulation of many questions of the public consultation does not adequately address the fact that most (if not all) online platforms thrive on processing of personal data. Instead, we note, throughout the text, references to "non-personal" data, to the effect of pre-empting respondents´ views on how *personal data* should be processed by platforms. We see this happen, for example, in the first question of p. 16,[1] which only mentions non-personal data, while the crucial issue concerns the transfer of personal data between online services. Regrettably, there are other examples in the text. Again, at p. 24, the questions reads "*In order to ensure the free flow of data within the European Union, in your opinion, regulating access to, transfer and the use of non-personal data at European level is...*". This question completely overlooks the fact that, when we think of online platforms, personal data are the most valuable information shared.

At p. 26 questions concern the "*Access and re-use of (NON-PERSONAL) scientific data*" and, again, the respondents are not given the opportunity to comment on the value that personal data have in the context of scientific research, but also on their commercial value to pharmaceutical businesses.

While we acknowledge that not all data stored and in transit on online platforms is personal data, we cannot help noting that a large part of it is and is also very valuable. The effect of having questions such as those mentioned in the examples is that important data protection issues are completely by-passed. In addition, the answers of respondents might be distorted

by the fact that they would like to, but cannot, refer also to the processing of personal data, with the consequence that the conclusion the Commission will draw from this exercise might be substantially flawed.

1. ***Definition of online platforms***

While admitting that adopting a comprehensive definition of online platform, given the diversity of business models, is a challenging exercise, the public consultation suggests, and seeks to test, a provisional definition.

We recommend including in the definition that online platforms entail the processing of personal data - a finalistic approach that highlights the central role of personal data for platforms.

Should the Commission opt for regulating platforms, such a definition would bring to the legislator´s attention data protection issues, such as *privacy-by-design*, accountability, transparency, user's control over their data (including data portability), security measures and other risk-mitigation techniques such as data minimization.

Last, we note that the definition excludes internet access providers (IAP), as a category, from the scope of the definition. We consider, in this respect, that a blanket exception would not work, as it might be the case that IAPs host on their websites online advertising, thus functioning as a platform connecting their customers with third-party advertisers. This business modality was more evident in the past -when many IAP also operated web portals with free services (e-mail, weather forecasts, stock prices) and online advertising-, but might still be used today.[2]

2. ***Transparency for users of online platforms: consumer and citizen protection***

Online platforms have set up business models, which (in the majority of cases) monetize the growing volume of personal data they collect through the provision of free services. The complexity of such business models increases the information asymmetry between service providers and customers. The latter, therefore, often find it difficult to have a full and clear understanding of the way platforms impact on their life and economic position.

Transparency is a fundamental principle of both consumer protection and data protection law (see, in particular, Article 8 of the Charter of Fundamental Rights of the EU). In the context of consumer protection law, transparency helps ensure equilibrium and fairness between the contracting parties (the provider and the customers). In relation to data protection law, transparency ensures that data subjects retain control on their personal data and on the way they are used. Under EU data protection law, platforms should provide clear information concerning all the terms of contractual arrangements they enter into with customers. They should also provide clear and transparent information as to the collection of personal data and its processing. In particular, such an obligation follows from the fundamental requirement of fair processing and affects the exercise by individuals of their rights to access, rectify and object.[3]

Our concern is that the current level of transparency in the processing of personal data is often insufficient and neither provides customers with a level of understanding of the processing of their data nor enables them to make informed choices. Transparency can help

ensure that consumers, once fully aware of the mechanics of data processing and monetisation, demand that their data be processed in a fairer way or switch to platforms that use their data in a fairer and more efficient manner.

From a policy perspective, transparency and the ability for consumers to switch between platforms are highly desirable features, as they may trigger a "race to the top", encouraging businesses to compete on the data protection standards they offer to their customers.

Online platforms should clearly display privacy policies that explain how personal data are processed and protected, by whom, for what purposes and how long they are retained. As customers might be reluctant to read long privacy policies, the latter should be drafted in plain and accessible language.

3. Use of personal data for legitimate and non-legitimate purposes

Pursuant to Article 6(b) of Directive 95/46/EC, personal data shall be collected and used for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. In this respect, the major policy concern is that online platforms have an economic incentive to use data for purposes different and potentially incompatible with the original purpose for which they were initially collected.

Online platforms also facilitate partnership between businesses that would not otherwise connect with each other. While this is an important economic function, it may make it difficult to inform individuals on how their data are going to be used.

It is important, in this respect, that platforms provide clear, *ex ante* information to customers/users about their business model and the role that personal data play in that context. If any element of data processing is not known (*e.g.* because new, unpredictable business partnerships form on the platform), the platform shall have in place technology that will timely notify users of any new processing of their data *before* it starts (*e.g.* notification mechanisms on smart devices) and enable them to react, if they so wish. In this respect too, *privacy-by-design* and *by-default* may help businesses to cater in advance for regulatory needs.

4. Tackling illegal content online

As a preliminary remark, we note that service providers (*e.g.* online platforms) that "host" (or store) content provided by one of their users benefit from a "mere conduit" exception under the e-commerce Directive. Such an exception, however, is conditional on the fact that the provider is not aware of the illegal nature of the content or, upon becoming aware thereof, takes action to remove or disable access to the content. Consequently, the exception should not apply when a violation of data protection rules is, or becomes, apparent to the platform operator (*e.g.* personal information is used for harassment purposes).

The Commission consultation rightly focuses on content, as the main driver to the success of a platform. While the technology infrastructures necessary to operate a platform are regulated and, in addition, subject to general competition rules, content use is largely subject to contracting dynamics between private parties. Hence, the need to establish when content is legal, and therefore fully negotiable, and when it is not.

While there is no (or little) doubt that content used in violation of copyright is illegal and mechanisms are put in place to 'police' copyright violations on platforms, we would like to encourage platforms to proactively put in place similarly effective protective measures (*e.g.* mechanisms for effective take-down requests[4]), when personal data processing does not comply with data protection rules. Linked to this issue is the question on whether platform operators should actively monitor the content stored on their online environment.

5. ***Competition between platforms and barriers to users´ switching***

Consumers´ ability to switch from platform to platform plays a crucial role in stimulating competition and innovation, including in the field of data protection safeguards, to the benefit of users.

In this respect, we consider that an obstacle may be linked to the absence of data portability, which implies the need to provide *ex novo* all the data subject´s personal data to a new platform. Data portability is a concept that we have repeatedly advocated.[5] As stated in the text of the public consultation, data portability is restricted whenever personal data are not fully accessible or are provided in a non-usable format. If the transfer of the personal data online is not available, technically difficult or costly, the users will be likely to confirm the initial choice they made. Ensuring data portability is therefore a key point to ensure fair competition between platforms, in addition to being a key enabler of user control. Standardisation activities supported by legislation or effective self-regulation are of paramount importance to support data portability and need to be fostered. At the same time, it is essential that the implementation of data portability not be hindered or postponed pending the results of any possible future standardisation and self-regulation, which may take a long period of time.

6. ***Internet of Things: functioning, safeguards and allocation of liabilities***

Almost all platforms operating online (*e.g.* Amazon, Google, Facebook, Ebay) develop software applications that run on users´ smart devices (*e.g.* phones, tablets, smart-TVs, watches.) with a large market penetration. Furthermore, products and objects supporting services offered through these platforms are more and more connected and can provide direct communication among them and feedback to the platform itself. All this contributes to the Internet of Things ("IoT")[6], which brings about a significant capability to "harvest" personal data on a large scale, coupled with increasing computing power ("big data").[7]

The interaction between IoT and big data may pose risks to data protection among others, because it allows establishing connections between seemingly isolated and unrelated information. In addition, generating knowledge from trivial data or even data previously thought to be "anonymous" will be made easier by the proliferation of sensors, revealing specific aspects of individual's habits, behaviours and preferences.[8]

This scenario appears even more complex, considering that connected objects are generally produced by various manufacturers, which, in turn, may either engage in data processing autonomously or entrust it to third parties. The market, therefore, may be (and actually is) populated by a multitude of co-controllers and processors, which make the allocation of responsibility and liability more difficult and may hinder data subjects in their ability to exercise their rights, be in control of their data and obtain redress.

The most effective regulatory response, in the above respect, consists of applying in a coherent way the Data Protection Directive, which identifies the controller as "*the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data*" and assigns to it the fulfilment of a number of duties designed to protect the individual´s rights to privacy and data protection. Therefore, before engaging into any data processing, platform operators and other service providers should identify themselves as data controllers (or co-controllers) in the information they provide to users whose data they process. They can identify their position as controllers based on the mere fact that they are processing personal data for their own purposes. This approach ensures that businesses act responsibly and in compliance with the Directive and that liability is efficiently allocated.

We would like to recall, to conclude, that in the *Google Spain* judgment, the Court has rejected the search engine´s attempt to escape liability for not fulfilling data protection obligations based on the fact that the processing of personal data took place on third-party websites (for their purposes).[9]

7. ***Personal data and cloud computing***

Since most online platforms are cloud-based, they share cloud computing challenges to personal data.

Despite the essential role cloud services play for the deployment of online services, EU consumers still do not seem to fully trust cloud-based services, and this for several reasons: uncertainties about effective data storage location and applicable law, lack of transparency on the security level guaranteed by the cloud provider and, last but not least, unforeseeable allocation of risks between the cloud provider and the user for data breaches and subsequent liability.[10]

As a result, finding privacy-friendly solutions for cloud computing services represents one of the main challenges for online platforms. The EDPS, on his own and as member of the Working Party 29 has already expressed his views in the past[11] and continues to offer relevant support and advice.

Boosting research and marketing of solutions increasing transparency and user's control over their data (such as "personal data management systems") is essential to offer a higher level of protection and thus increasing users' trust.

Cloud-based platforms may also engage into data transfers to third countries, triggering the need to ensure an adequate level of data protection as required by the Directive. The receiving country, in particular, shall provide data protection safeguards essentially equivalent to those guaranteed within the European Union framework, as confirmed by the ECJ´s recent case law.[12]

Conclusion

The most important comment we have, in reply to the Commission public consultation, is the need (if not the urgency, considering the pace at which platforms develop) to properly define the relevant questions concerning the use of personal data on online platforms. In this respect, limiting questions to "non-personal" data only results in circumventing or deferring problems,

with the consequence of building policy on erroneous (at best, incomplete) considerations. Any future instrument must be based on the premises that personal data are very likely to be processed. A simple reference to the GDPR may not be sufficient to provide legal certainty, so a thorough reflection is needed as to how precisely incorporate data protection requirements into the EU policy on online platforms.

In terms of regulatory approach to data protection issues, we consider that the existing data protection principles and rules (on necessity, proportionality, data minimisation, purpose limitation and transparency) complemented by new principles (such as accountability and data protection and privacy by design and by default), as a consequence of the data protection reform, will provide a sound basis for the safeguard of individual´s right to privacy and data protection. Increased transparency, adequate rights of access and data portability and effective opt-out mechanisms may allow users more control over their data, and may also contribute to more efficient markets for personal data, to the benefit of consumers and businesses alike. Greater penetration of data protection principles in sector-specific legislation will also be necessary.

Good regulation, however, while essential, is insufficient. Companies and other organisations that invest a lot of effort in finding innovative ways to make use of personal data should use the same innovative mind-set when implementing data protection principles. What remains necessary is a steady adoption of privacy-enhancing solutions that can compete in the market, transparent and effective self-regulation by the industry building upon legal principles and technical standards and a greater level of education and awareness for users and providers.

Done in Brussels, on 16 December 2015

[1] The question reads "*Should there be a mandatory requirement allowing non-personal data to be easily extracted and moved between comparable online services?*"

[2] See, for example, the website tiscali.it

[3] See ECJ judgment of 01.10.2015, in case C-201/14, *Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate and Others*, paras 33-34.

[4] See ECJ judgment of 13.05.14, in case C-131/12, *Google Spain v AEPD*, where the Court found that the search engine has to erase information that is no longer relevant, or excessive in relation to the purposes of the processing (para 94).

[5] See EDPS Opinion 7/2015, "*Meeting the Challenges of Big Data*", available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf; Opinion 4/2015, "*Towards a new digital ethics: Data, Dignity and Technology*", available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-11_Data_Ethics_EN.pdf and Opinion of 26 March 2014, "*Privacy and competitiveness in the age of big data*", available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf.

[6] See Article 29 Working Party Opinion about the Internet of Things ("Opinion 8/2014 on the Recent Developments on the Internet of Things"). "*The concept of the Internet of Things (IoT) refers to an infrastructure in which billions of sensors embedded in common, everyday devices – "things" as such, or things linked to other objects or individuals – are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities*".

[7] Particularly relevant, in the above respect, are wearable computing devices (e.g. watches, glasses, bracelets, music players, t-shirts) which embed multiple interconnected sensors capable of recording behaviour, body functions and lifestyle information.

[8] See Article 29 Working Party Opinion about the Internet of Things, p. 8. Platforms, providers of apps and smart devices may gather data sufficient to build group-specific statistics (corporate-wide profiles or regional profiles) on any users´ parameter for themselves or their partners (e.g. corporations or governments). This may create for platforms, service providers and other market players with access to data an incentive to move from supporting users in their self-quantifying (e.g. the possibility offered to users, generally for free, to measure their health parameters) to voluntary smart coaching (e.g. allowing users to follow a healthy lifestyle with advice from a third party) to a phase where they may rely on behavioural scientists to "push" the "right" message onto users at the "right" moment, thus influencing users´ behaviour.

[9] See ECJ judgment of 13.05.14, in case C-131/12, *Google Spain v AEPD*, paras 22 and 28 ss.

[10] See EDPS Opinion of 26.11.2012, on the Commission's Communication on "*Unleashing the potential of Cloud Computing in Europe*", available at https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf

[11] See the Opinion of the Article 29 Working Party of 22.09.2015 on the Code of Conduct on Cloud Computing, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf and the opinion of 01.07.2012 on Cloud Computing, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

[12] See ECJ Judgment of 6.10.2015 in case C-362/14 *Maximillian Schrems v Data Protection Commissioner*, paras 73-74.