FP7-SSH-2009-A
Grant Agreement Number 244643
Collaborative Project CONSENT

Interoperability: The Impact of Commission's Proposed Data Protection Regulation
Appendix to Deliverable D5.1

Revised:	Andrej Savin	1/7/2012
	Andrej Savin	1/9/2012

Introduction

The European Commission recently proposed a General Data Protection Regulation,[1] which is meant to replace the EU Data Protection Directive[2] and to thoroughly reform and modernize the EU privacy regulatory framework.

The Regulation, if adopted, would introduce a number of changes, several of which would considerably alter the current privacy setting.[3] First, the current Directive would be replaced with a Regulation, achieving EU-wide harmonization. Second, the scope of the instrument would be widened and the provisions made more precise. Third, the use of consent for data processing would be limited. Fourth, Data protection "by design" would be distinguished from data protection "by default". Fifth, new fundamental rights would be introduced and the old ones clarified. Sixth, new rules on controllers' and processors' duties, on supervisory authorities and on sanctions would be introduced. Finally, the Commission would obtain significant new powers to adopt delegated acts.

This appendix explores the impact that the proposed Regulation might have on interoperability of user-generated services.[4] Since the proposed Regulation is an

1 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of data (General Data Protection Regulation), COM(2012) 11/4 draft (including explanatory memorandum).
2 Directive EC/95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31
3 See Hornung, G., "A General Data Protection Regulation for Europe? Light and Shade in the Commission's Draft of 25 January 2012" (2012) 9 ScriptEd 64 and Kuner, C., "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law" (2012) 11 Privacy and Security Report 6
4 The text assumes the adoption without any amendments – which is, in reality, an unlikely option.

instrument of high complexity, only those provisions of direct relevance for the project and Work Package 5 will be analysed here.

Possible impact on interoperability

Sphere of Application

The Regulation's scope of application is covered in Article 3 paragraph 1 of which provides that it applies to "the activities of an establishment of a controller or a processor in the Union." This is a situation involving a corporation operating within the borders of the EU. Article 3(2) further provides that the Regulation will apply to "the processing of personal data of data subjects residing in the Union by a controller not established in the Union" in two distinct circumstances. First, where goods or services are offered to a data subject in the Union or, second, where data collection relates to monitoring of data subjects' behaviour. Thus, an American UGC service accepting registrations from EU users would fall within the scope of the EU Regulation.

The Directive's scope of application is narrower. In situations involving controllers situated outside the EU, the Directive only applies where the controller uses equipment located in the EU (Article 4(1)(c). A user-generated website (UGC) established in the United States but providing services globally, including in the European Union, will only be covered in the Directive if the rules of private international law lead to the application of the law of a Member State[5] or if the equipment used for processing is located in the EU.[6]

A large number of UGC websites targeting EU customers are located outside the European Union. At the same time, the most popular ones (Facebook, Youtube, Twitter, Wikipedia, etc.) are all established in the United States. Such websites often either do not have any establishment in the EU or only have offices which conduct marginal or local business, thus making the application of the Directive unlikely. In light of these facts, the revision of the scope of application in the Regulation is to be welcome, as it will include a number of websites popular among EU users.

Fundamental Concepts in the Preamble

5 Article 4(1)(b)
6 Article 4(1)(c)

In the Legal Report (Deliverable D5.1)[7] and the Impact Report (Deliverable D5.3)[8] it was emphasised that enabling interoperability between UGC websites requires both the data subject's *consent* and a clear explanation of the exact *circumstances* in which data is transferred between two UGC sites. The reports also emphasized that the most widespread form of interoperability is the ability to log into one account using the credentials of another.

Interoperability of user-generated websites is a well-implemented reality which improves users' experience by enabling them to access more sites with fewer IDs and exchange information between various services. At the same time, it increases the potential for privacy violation by decreasing the users' control over who has access to information and under what circumstances. What changes does the new Regulation bring concerning interoperability?

The Regulation redefines the concept of *consent* as a basis for processing data. paragraph 30 of the Preamble says that purposes for data collection should be "explicit and legitimate" and "determined at the time of the collection." This would suggest not only that the data collector/processor needs to be open about any interoperability issues but also that any communication to users/subjects needs to be performed at the time when the data is submitted and not later. Paragraph 31 provides that consent is *one* of the legitimate bases for processing but that other bases laid down by law either in the Regulation or in EU or national law can also serve the same purpose. In this, the Regulation is not fundamentally different form the Directive.

If data had been processed with the data subject's consent, the burden of proof that the consent had been obtained, according to paragraph 32, is on the data controller. This is an important if indirect improvement, as it suggests that consent should never just be *assumed* but must rather always be well *documented*. No similar provision exists in the Directive.

A fundamentally new concept, the Right to be forgotten, is introduced in the Regulation. This right, first mentioned in paragraph 53, provides that data subjects shall have the right to have their data *rectified* or, in cases where collection is not in compliance with the Regulation, *erased*. This is in particular the case where processing is no longer necessary, where consent had been withdrawn or where the data subject raises objections to processing.

In terms of UGC websites, this policy allows an account holder to withdraw consent to data processing for reasons concerning interoperability features at any point during his use of the UGC service. Therefore, if an account holder determines that more information is shared with other UGC websites than envisaged in the original consent, a simple request to the UGC provider should be able not only to suspend or terminate the account but also to erase the data which the UGC site as controller maintains at the point.

7 See Deliverable D5.1, section 2.5
8 See Deliverable D5.3, section 2.3

Of particular interest for interoperability issues is paragraph 57 which allows objecting to data processing in situations involving direct marketing. This right, previously present in Directive Article 14, has now also been transferred into Preamble. Objections must here be made possible without charge and in an effective manner. This would cover situations where data controller made the web site interoperable with other sites which primarily do direct marketing or rely on such marketing.

Consent and other bases for processing

The Regulation takes significant steps towards making consent a clearer and more stable basis for legally processing data. This is done through clarifying the definition of consent as well as making the conditions for obtaining it more stringent.

Article 4(8) defines consent as "freely given specific, informed and explicit" indication of his or her wishes by which the data subject, "either by a *statement* or by a *clear affirmative action,* signifies agreement to personal data relating to them being processed." The Regulation provides more detail here than the Directive, clarifying the position by providing that consent can be given either by a simple statement, which includes e.g. the clicking of a button "I agree" or similar, or by other "clear affirmative action." The requirement that action be "clearly" affirmative removes the possibility that simple silence or consent given for previous different services by the same company might serve the purpose.

In addition to this, a new requirement has been introduced in the Regulation Article 4(8), spelling out that the consent needs to be "explicit." This is of direct importance for interoperability as it would mean that the user must explicitly agree to any interoperability features, not only in relation to the what UGC data will be shared with but also in terms of features and functionality that the said UGC might provide.

Further supporting this position is Article 5 of the new Regulation, which adds a new condition for data processing in relation to the Directive. It provides that data must be processed not only lawfully and fairly but also in a "transparent manner". This reflects the importance of transparency in the Regulation, which is further emphasized in Article 11.[9] By analogy, transparency also needs to exist in relation to the consent.

A third clarification in relation to the nature of the processing and, through it, the consent, is found in the principle of data minimization of Article 5(1)(c). This provision introduces the principle of data minimization requiring that only data

9 The word has been used no less than 15 times in the Regulation, compared to only once in the Directive.

absolutely necessary should be collected. By analogy, data minimization requires applied in relation to interoperability would require that the minimum data only be transferred to interoperable websites.

Article 7 clarifies the conditions for consent which in the Directive were regulated in a cursory manner only. Importantly, the burden of proof that data subject's consent had been obtained shall be on the controller and must relate to "specific purposes". In cases where the consent is obtained as part of a written declaration on another matter, the Article provides that consent for data processing must be given in a manner distinguishable from the other matter. The consent can, according to Article 7(3) be withdrawn at any time.

A special provision is inserted in paragraph 4 to invalidate the lawfulness of processing based on consent in cases where an "imbalance" exists between the subject and the controller. This is clarified in the Preamble paragraph 34 as including the employers' gathering of data on employees and certain cases where the public authorities gather data about citizens.

The new article has an indirect but important impact on interoperability. The burden of proof requirement coupled to specificity of purpose serves to discourage transfers which rely solely on previous unrelated consent. In other words, an operator of an UGC site which decides to engage in interoperability at some point *after* the user had given general consent cannot, on being challenged by that user, rely on the general consent (most likely obtained at sign-up time) but must prove that a specific consent has been obtained.

Similar to the Directive Article 7(f), an exception in Regulation Article 6(1)(f) provides that consent is not needed where "processing is necessary for the purposes of the legitimate interests pursued by a controller" except where these are overridden by fundamental rights and freedoms of the data subject. Contrary to the Directive, the legitimate interests are those of the controller only and not also of the third party. It is not entirely clear what the legitimate interests of controllers are but it might be reasonably surmised that they may involve such fundamental interests as freedom of expression.

Article 9(1), which relates to processing of special categories of data, clarifies the position in the Directive by adding genetic data and data relating to criminal convictions or related security to the list of special categories. The additions have no particular bearing on consent obtained in interoperability situations.

Article 11 of the Regulation requires transparency and accessibility of policies with regard to processing of data and the exercise of data subjects' rights. Any communication relating to subjects' data shall be in an "intelligible form" and written in "clear and plain language" adapted to the data subject.

In interoperability situations, this would mean that any information concerning interoperability, including the relevant sites, the data transferred including the circumstances, the time and the scope, must be communicated clearly. The ease

of access would further mean that the information must be clearly visible, probably in the form of general terms of use.

Information and Access to Data

The Regulation Article 14 widens the scope of information which needs to be made available to the data subject both for situations involving direct access to subject's data (Directive Article 10) and data obtained from other parties (Directive Article 11). This information now includes, among other items, contract terms and general conditions (Article 14(1)(b)), the period for which data will be stored (Article 14(1)(c)), the existence of the right of rectification (Article 14(1)(d)), the right to complain to authorities (Article 14(1)(e)), the recipients of data (Article 14(1)(f). Unlike the Directive, which only made the information on the identity of the controller and the purposes obligatory, these conditions are mandatory and not only provided where "in so far as such further information is necessary."

The information requirements are significant for interoperability situations. In the Directive, in a situation where UGC A receives data from UGC B, the latter need only disclose the identity of the recipient and the purpose. Having received the information, UGC B then may have to disclose further information but only "in so far as such further information is necessary."

In the Regulation, in the same scenario, Article 14(3) makes it mandatory for both controllers A and B to provide the full spectrum of information to the subject.

In terms of access to data, the information the data subject can demand from the controller in Directive's Article 12 has been extended significantly in Regulation Article 15. Among other things, paragraph c of that article provides now that "the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries" can be demanded. This means that a user concerned about data transfers in interoperability situations can demand both from the sender and the recipient controllers information regarding who exactly will receive data even in situations where UGC providers are based overseas (as they often are).

Right to be Forgotten

Regulation Article 17 introduces the right to be forgotten in a much wider scope than the previous Article 12(b) of the Directive. This consists in the right to have the information held erased and the right to demand cessation of further

dissemination of such data. The obligation is made particularly strong where data had been collected while the subject was a child.

In terms of interoperability, the request to erase data would not only allow the data to disappear from the controller's servers but also to prevent the transfer of information to other UGC websites. If a UGC is being merged with another one or taken over, such a request would have the effect of "sterilizing" the data.

The Regulation is not clear about whether the data need to be physically erased (i.e. all traces removed) or simply made permanently inaccessible to third parties. Although the word "erase" implies physical destruction of data, the actual wording in the article leaves scope for other interpretations, especially as paragraph 8 says that, where erasure is carried out, the controller should not "otherwise process such personal data," implying that they are still available on the server.

There are four grounds on which data shall be erased. This is where data is no longer necessary, where consent had been withdrawn, where the right to object had been exercised or where the processing does not comply with the Regulation.

Where the controller had made the data public (as may often be the case with UGC users' profile pages), that controller has the obligation to inform "third parties which are processing such data" that consent had been withdrawn. This may be the case where public UGC profiles had been recorded by another UGC and pre-packaged for those users who wish to reactivate them on these other websites.

Right to Portability

Article 18 of the Regulation brings a new right. ""Where personal data are processed by electronic means and in a structured and commonly used format", the subject has the right to obtain a copy of data for further use on another website.

This is a form of interoperability which we have labelled "software interoperability" in D5.2. This means that underlying platforms on which various UGCs operate are able to communicate with each other.

It is, at present, not clear to what extent the users may be interested in this kind of interoperability. Deliverable 5.2 demonstrated that social graph interoperability was non-existent. In other words, none of the UGC sites analysed allowed the user to "transfer" the list of friends and their respective interconnections. This should not be taken as an indication of the lack of interest on the users' side but rather as strategic behaviour on the side of UGCs themselves.

The present article gives legal ground for this kind of platform interoperability but presupposes the existence of a "commonly used format". As there is no such format at present point, it remains to be seen whether this article will really bring any changes in the interoperability picture.

Profiling and Data Aggregation

Profiling is a form of dynamic analysis of the user based on finding patterns or correlations in large pools of data. The *interoperability* significance of profiling is in the fact that it enables larger pools of data, thus increasing the effectiveness and, indirectly, commercial viability. Put in different terms, two or more interoperable UGC websites contain a larger user base thus increasing the pool of information which can be used for profiling but, indirectly, also the potential threats. For example, when a regular UGC (i.e. a general social network) becomes interoperable with a dating UGC, the sexual preferences available in the latter may become apparent in the former with little or no control on the users' side.

The phenomenon is already covered in Regulation Preamble, paragraph 58, which limits profiling based on automated processing. Regulation Article 20 builds on Directive Article 15 but increases the control mechanisms and makes conditions for profiling more stringent. Data subjects natural persons have the right to object to profiling. Here, as elsewhere, consent plays a crucial role as profiling may be allowed where it is given prior to the action taking place. Nevertheless, profiling is allowed in the course of entering into or performing a contract, where proper safeguards have been taken.

It is submitted that the Regulation does not go far enough in protecting data subjects. This is a result of the nature in which modern information is gathered on the Internet. While individual pieces of information may, on their own, not be of any relevance and may not make the data subject vulnerable, taken together they may represent a significant threat. For example, a photograph put on Flickr may be geo-tagged, easily connected to a UGC site which contains general information (including, possible, address, email and telephone number) and further linked (automatically or not) to other UGC sites. While it is true that Article 20 may serve to control profiling taking place in the open, it does little or nothing to prevent the aggregation of information.

Transfer of Data to Third Parties

Transfer of data to third parties, already regulated in the Directive Chapter IV has been more precise and, in places, more stringent. This section will be relevant in situations where UGC website in the EU is interoperable with a UGC website outside of the EU.

Conclusion

The new Regulation would, if adopted, bring welcome changes in situations involving interoperability in all aspects identified in D5.1 (account, content and software interoperability).

Of particular importance is the more precise and more stringent regulation of consent, which is the most relevant basis for legitimate processing of users' data. This ensures that users are aware of all the relevant circumstances at all stages of the transaction, in particular at points where they have not previously consented to their data being given to third parties.

Also relevant are the new provisions on data anonymization and profiling. On the other hand, it is to be regretted that more has not been done to protect users in situations involving data aggregation.

In conclusion, the new Regulation is a somewhat better instrument for protecting users in situations involving interoperability.