STUDENT FORUM
MAASTRICHT

Policy Proposal on

Data Protection and Digital Single Market

Data Protection Revised: A Focus on Enforcement and Public Awareness

Brussels, April 19th 2015

Authors: Martina Baraldo, Lucas Barrios, Camille Maye, Charlotte von Knobloch, Mirta Cavallo, Dominik Hertlik, Kateryna Hnativ, Viktoriia Paimanova, Valeriia Sofishchenko, Edyta Stopyra

Tutor: Dr. Giuseppe Mazziotti

STUDENT FORUM MAASTRICHT

Student Forum Maastricht (SFM) is an annual student conference held at the Maastricht University Campus in Brussels. The conference is organised by students from Maastricht University in cooperation with different partner organisations. The participants are post- and undergraduate students from all over Europe with diverse academic backgrounds. Based on problem statements provided by European Commission representatives, they develop policy proposals for pressing topics within the Commission. In this process the students receive input and insights from experts from NGOs, academia and the business sector working in Brussels. The 2015 edition of SFM took place from 15th to 19th April. In five different working groups policy recommendations were drafted dealing with the following topics: EU Energy Union, EU Asylum Policy, Independence of Regions, EU Minimum Wage Policy, and Data Protection & Digital Market. For more information on Student Forum Maastricht, please visit: www.student-forum.eu

Content

Executive Summary

The issue of data protection plays a particularly significant role with regards to the next-to-come Digital Single Market as part of the EU's Digital Agenda. Various incidents including the EU antitrust case against Google as well as the international scandal concerning the NSA's monitoring activities have led to outrage among EU citizens and shifted the public focus on privacy-related rules of the digital sphere. Currently, the issue of data protection has generated strong public controversies.

This proposal focuses mainly on the effective enforcement concerning the fundamental right of privacy due to the existence of a new regulation on data protection policies drafted by the Commission. Still, the proposal aims a introducing various recommendations including

- raising public awareness regarding the digital sphere
- simplifying the users' exercise of rights through user-friendly mechanisms
- the creation of best practices developed with the support of consumer associations & personal data controllers under the supervision of DPAs
- the harmonization of the DPAs competences & enhancement of cooperation between the Member States' DPAs
- the creation of a supervisory body (i.e., a European Data Protection Board)
- launching of a Leniency Program to encourage companies to cooperate with EU institutions by providing the authorities with information on privacy infringement & proofs

The working group stresses that any final policy needs to be evaluated in the light of several objectives consisting of the right balance between human rights & market values, increased public awareness, effective enforcement and, lastly, technological neutrality.

Problem Statement

The problem we are facing is *"How can the Digital Privacy of EU citizens be maintained while enabling the free flow of data in order to achieve the goal of a Digital Single Market?".*

This problem is particularly relevant nowadays in the perspective of the next-to-come Digital Single Market as part of the Digital Agenda for Europe. It represents an important objective that – if achieved – can consistently foster growth. One of the main issues today is that citizens are unsure about how their data is concretely collected, used and made available to third parties for commercial purposes. Public awareness about online privacy issues has recently increased as a result of the EU antitrust case against Google and the international scandal concerning the monitoring activities of the National Security Agency.

Background

The function, which data protection plays in the context of the Digital Single Market, is complex and needs to be investigated from different perspectives while considering the impact of privacy-related rules on various business sectors. The exponential growth of the digital environment has made it urgent to upgrade the existing rules applying to individuals, but also to businesses, the public sector and supervisory authorities.

Guaranteeing trust online is an important concern for citizens: 70% of them are concerned that companies may use the personal data for purposes which are different from the ones for which they have collected it legitimately (i.e., with the consent of the individuals concerned). Only 26% of the social media users and 18% of online shoppers feel in complete control of the information disclosed.

The acquisition of digital skills by citizens and the improvement of business' digital performance are expected - by 2020 - to create 500.000 jobs, enable a € 250 billion growth and lead to a €500 million investment in cyber security and privacy-enhancing technologies. The countries' integration of digital technology is coherent with the amount of consumers purchasing online. The gap between world digital leaders in online-shopping such as Norway (73%), UK (71%), Sweden (71%), Denmark (70%), and low performance countries such as Bulgaria (7%), Romania (6%) is increasing. Additionally, personal data and big data collected from consumers' (online) activity have gained substantial economic value to companies, as they can reveal consumer habits, beliefs, interests and conditions. Hence, there is an increasing concern in the way that data is transferred (or sold) to third parties other than the original data collector (e.g. insurance companies, banks, heath services, marketing agencies etc.).

The reform plan of the existing legislation on developing data protection policies in form of a new regulation is supposed to have a general application. At the same time it raises problems with regard to the role and desirability of the ePrivacy Directive, which solely applies to the telecommunication sector. The co-existence of several legislative layers might create uncertainties because of overlapping provisions being applied to the same cases. Moreover, this might lead to interpretative difficulties, unequal treatment of different business sectors, and expensive and time-consuming disputes.

Objectives

(1) Human Rights vs. Market Values

Data protection as a fundamental right needs to be ensured while giving the market the opportunity to develop technologically and enhance innovation in order to grow. Citizens' trust is necessary in order to foster the flow of data, which is the very basis of digital economy.

(2) Public Awareness

Most citizens use the internet on an everyday-basis without sufficient knowledge on which data are monitored through cookies, collected and processed. Some of the most relevant phenomena are profiling, targeted advertisements and cookies. Besides the collecting of personal data, open data is also being processed through algorithms in order to gain more information about citizens' lives, behaviours and interests. This raises contradiction with regards to the respect of privacy rights and data protection, which is necessary in order to achieve the economic, political and social benefits of the Digital Single Market. Hence, more transparency is needed.

(3) Effective Enforcement

Meanwhile existing bodies of law have already consecrated principles protecting data and private life. The major issue concerns their effectiveness. It is therefore important to guarantee a better enforcement of those rights

(4) Technological Neutrality

Innovation is constant and unpredictable. In order to be effective, rules should be technologically neutral. Controllers of personal data should be made subject to the same rules, irrespectively of the kind of technology services. The convergence of media, technologies and services makes it difficult to justify the existence and development of sector-specific legislation, which covers just certain industries (e.g., the telecommunication operators).

Policy Recommendations

Raising Public Awareness

The European Union shall promote means which allow citizens to regulate the outflow of their personal data. It could be achieved through launching initiatives such as the release of sensitizing videos on social media, the publication of teaching materials for schools, organization of sensitisation courses and the sponsoring of technological solutions fostering privacy awareness and protection. These initiatives should target all population strata, with special consideration of 'digital immigrants', who are not familiar with modern technological means.

Simplify the Exercise of Rights

Data controllers should make accessible mechanisms (e.g. user-friendly forms) available to users in an easy manner allowing for the request of access, modification and removal of users' personal data. In the assessment, account should be taken of privacy infringement and situations where data controllers did not contract directly with the data subject. The data controller should provide a justified response to the user request of removal in a reasonable period of time.

The new regulation should require further protections from data controllers. As similar to the requirement of agreeing to Terms and Conditions, there should also be a separate consent requirement (e.g. tick box) relating specifically to data processing, usage and sale. Furthermore an obligation of notification of any change to the privacy and data processing settings should be enacted.

Best Practice

From a policy-related perspective, it is not wise and forward-looking to incorporate excessively detailed rules covering newly emerging situations, disputes and practical problems in an EU regulation. The effective implementation of the rights and obligations set out in such a regulation could widely rely on best practices and codes of conduct, which should be developed by Internet user and/or consumer associations as well as personal data controllers under the supervision of DPAs. Considering that large data processors and controllers tend to exploit each regulatory vacuum to disregard data protection obligations without having to bear consequences and sanctions, the aforementioned codes of conducts and EU-wide best practices would ensure that companies adopt and comply with the same standards. In light of their investigative and sanctioning powers, national DPAs might usefully exert their influence in order to control and encourage standardisation of best practices aimed at solving newly emerging problems or achieving a certain enforcement goal.

Structure, Activities and Powers of Data Protection Authorities

The proposed Regulation is expected to establish a 'one-stop-shop' mechanism, which will make it easier for individuals to have their rights recognized and implemented. Several measures should be taken to enhance cooperation between national DPAs and a newly created supervisory body (i.e., a European Data Protection Board), whose mission will be to ensure that the 'one-stop-shop' mechanism works effectively. In particular, the EU should:

1. Ensure that the competences of DPAs are effectively harmonised:

   DPA's competences enabling them to deal with Data Protection violations, and the extent to which they put them into practice, broadly differ across the Member States. It would be important to ensure that the proposed Regulation incorporates those competences, specifying that national authorities exercise such competences (and

the related sanctioning powers) in the same way. In particular, national DPAs should be entitled to issue warnings and impose fines that are proportionate to the gravity of violations and have a deterrent effect on data controllers. In order to avoid so-called 'forum shopping', it is necessary to ensure that national DPAs exercise their monitoring powers in a consistent manner.

2. Facilitate effective cooperation and consistency mechanisms (e.g. mutual assistance) between national DPAs with regard to cases within the EU dimension
3. Ensure that the European Data Protection Board exercises effective control over national DPAs

Strong supervision should be exercised by the European Data Protection Board with regards to the consistency of the task to impose sanctions by the national DPAs.

4. Ensure that the national DPAs are provided with a sufficient budget
5. Clarify the relationship and competences of the DPAs in the Member States with a federal system and coordinate the enforcement of the 'one-stop-shop' mechanism

There are also several de lege ferenda proposals that should be taken into consideration. We are however aware that they may be seen as very controversial and implementing them may be very difficult from the political perspective.

Uniformity of the DPAs Competences

A technological neutral approach should be adopted concerning the competences of the national DPAs. There should be no distinction between internet and telecommunication sectors with regard to the control exercised by the DPAs.

Broadening of the Competences of the European Data Protection Board

The Pan-European data protection body should be created with an analogical role as played by the European Commission with regard to the antitrust cases. Criteria to distinguish cases possessing a European dimension should be strictly specified.

Launching of a Leniency Program

A leniency program is already being used successfully in several fields, such as Antitrust Law. In transposing this policy to Data Protection, the European Data Protection Board - along with domestic authorities - should offer entities, which commit data protection violations, total immunity from fines or a reduction of penalties. As a consequence, companies would be encouraged to cooperate with EU Institutions by providing the authorities with insider information on privacy infringement and proofs. This would trigger a chain reaction and reduce the amount of infringements in the long term. As instance, the first company to co-operate and satisfy the formal requirements would be granted a total immunity from fines, while companies that co-operate subsequently would be granted a reduction on the amount of the fine up to 50%. Moreover, if companies are induced to cooperate, the competent data protection authorities would

save resources, which could be used for other privacy-related activities. In order for the leniency program to be effective, a necessary prerequisite is to ensure that the DPAs' investigative and sanctioning powers are substantial. Otherwise it would be an empty threat.

Conclusion

Considering that there will be a new regulation on data protection policies enforced at the end of 2015, this proposal mainly focuses on its effective enforcement with regard of the fundamental right of privacy. The Data Protection Authorities need to fulfil their role with regards to enforcement and their cooperation needs to be harmonized. In times of expanding digital markets and exponential technology development, the proposal gives the recommendation to raise the public awareness of European citizens in order to have sufficient knowledge on the collection and processing of their personal data. This includes the possibility of simplifying the ways in which EU citizens can exercise their rights with regards to privacy and data protection.