Limitations (Articles 6, 8, 9 and 20 of the Regulation)

Introduction

Articles 6, 8, 9 and 20 of the draft Regulation contain a number of important rules regarding the processing of personal data. These articles determine the legal grounds for processing, the grounds for processing data of children, rules for the processing of special categories of data and rules for the profiling of data subjects. These rules, in particular articles 6 and 20, must set significant minimum safeguards as to the lawfulness of both offline and online processing including for the profiling of data subjects. Data subjects as well as data controllers will both benefit from such strong rules, as they keep data processing fair, predictable and transparent and provide certainty and guidance. The online environment in particular needs strong and clear rules to ensure and, increasingly, to restore trust in online services. Trust is an important condition for the growth of the online sector.

EDRi broadly welcomes the fact that these important articles provide at least a similar level of detail as Directive 95/46/EC. However, the number of limitations to the important principles enumerated by these articles maintain existing loopholes and create new gaps in the protection of personal data. This paper outlines these limitations and describes the problems that they cause. In conclusion, we propose amendments to address these flaws.

Article 6(1)(f), legitimate interest as a legal ground for processing

Article 6(1) defines six grounds for processing of personal data. Legitimate interest currently serves as the basis for virtually unrestricted and unregulated forms of data processing. Examples of these forms of such data processing include direct marketing, fraud detection, monitoring of employees and further use of data originally collected for other purposes.

Using the legitimate interest justification for data processing is appealing for data controllers, because this basis does not carry the same obligations as the other legal grounds included in article 6(1)(a) through 6(1)(e). Legitimate interest allows data controllers to process personal data of data subjects for any purpose, provided that the processing serves a 'legitimate interest' and that the interests of the controller are being *balanced* against the interests or fundamental rights and freedoms of the data subject. However, data controllers will naturally give more weight to their own interests than to those of data subjects. It can therefore not be left to the controller to balance its interests with those of data subjects. It is impossible to verify if the 'balance test' in fact took place as few data subjects have yet been able or willing to test reliance on this criterion in court. This gives data controllers the freedom to let their interests prevail over the theoretical interests of data subjects, causing a serious imbalance. In short, the legitimate interest ground is very broad and its proper use is hard to verify. This leads to uncertainty regarding the scope and lawfulness of certain forms of processing. The more thorough safeguards included in the other grounds for processing suggest that this loophole will be used by even more data controllers in the future.

The online environment has seen a number of cases where data processing was extremely hard to understand and assess. Google's merging of data privacy policies across all its services is one of

these examples. The investigations lead by the CNIL have not yet resulted in a clear ruling on the lawfulness of these practices, which are extremely hard to grasp for the average user. In the US, the Federal Trade Commission has four large online multinational companies, namely Google, Facebook, Twitter and Myspace under 20 years consent decrees, requiring them to liaise with the FTC in case of changes to the way they handle the personal data of their users. This measure was introduced as a result of unlawful processing in the past. EDRi firmly believes that such incidents will lead to a decrease of trust in online services, which is why such situations must be prevented in the EU, by avoiding further unrestrained use of the legitimate interest clause. We therefore suggest amending article 6(1)(f) to achieve the following outcomes:

- Specifically exclude direct marketing as a 'legitimate interest'. Article 6(2) in the interservice draft required consent for direct marketing, which provides a better balance between the rights of data subjects and data controllers. It would also bring this Article more in line with the e-privacy directive, which requires consent for direct marketing and consent for online behavioral advertising. It seems illogical to set lower standards for offline direct marketing. It should also be noted that direct marketing techniques changed significantly since the adoption of the 95/46/EC Directive. Today “direct marketing” often refers to complex and intrusive activities performed by data controllers, such as the use of advanced profiling techniques, behavioral advertising and very precise targeting schemes (sometimes leading to price or service differentiation). It is essential to educate users and increase their awareness of how direct marketing may affect their private life. In this context the requirement of obtaining informed consent may play a vital role to the benefit of the data subjects
- Data subjects should be able to object (opt-out) from any form of processing based on legitimate interest. Opting out must be directly effective and free of charge. Objection must be possible at any moment, including the moment of collection of personal data, via the same channel as the data are being collected or the direct marketing is being sent. Recital 38 as well as Article 6(5) must be amended to achieve this and no longer contain a reference to 'specific situations' as a prerequisite for objection based on legitimate interest.
- Clarify the meaning of the 'legitimate interest' provision in the preamble. Recitals should clarify what will be considered legitimate interests, define the notion of data subjects' interests in more details and clarify how these interests should be weighed or verified.
- Clarify that public authorities cannot rely on Article 6(1)(f) as a ground for lawfulness, in line with recital 38. The current drafting is unclear.

Article 6(4): further non-compatible use of personal data

Purpose limitation is one of the pillars of data protection law. By specifying for which specific purpose data are being collected and used, it is possible for data subjects to give their informed consent or object to such use. Directive 95/46/EC established that data could only be processed further, e.g. for other, new purposes, provided that such further use is *compatible* with the original purpose and the data subject is informed about such use. This requirement keeps data processing fair, transparent and predictable.

The Regulation, in article 6(4), leaves this principle behind and states that further use of personal data is permitted, even if such use is *incompatible* with the purpose for which the data had originally been collected. As stated in the previous paragraph, this damages the very basis of data protection and is inconsistent with one of the fundamental principles of data processing as laid down in article 5(b) of the Regulation, which states that data cannot be processed further for incompatible purposes, be that by the controller or a third party.

Legitimizing further non-compatible use of data will inevitably lead to situations where data subjects are confronted with unexpected instances of such of further use. For instance, one can imagine a case when a data subject has provided his or her data in order to conclude a contract and subsequently finds out the data are further used by this company in order to exercise 'public tasks'. Allowing incompatible use is not transparent, not predictable and not fair, as it creates uncertainty for data subjects and too much leeway for controllers to use, re-use, combine and transfer data to other parties without restrictions or without being bound to the purpose for which the data were originally collected. Especially in a time where the collection of personal data has greatly increased, and where it becomes more and more clear that personal data are becoming a commodity, the processing thereof must adhere to the principle of purpose limitation. EDRi strongly recommends that article 6(4) be deleted and replaced with guidelines setting the boundaries of compatible further use of personal data.

Article 8: processing personal data of children

The extra protection of minors as provided by this article must not implicate the need to collect even more data for the mere purpose of determining the age of a child. Secondly, rules for the processing of personal data of children, including methods to obtain verifiable consent, must apply alike for enterprises of all sizes. Relieving smaller enterprises will lead to a gap in the protection of minors given the fact that company size does not relate to the number of records of data subjects (including minors). Furthermore, the size of a business in the digital environment often has little or no relationship to its financial power – the selling of Instagram – which had only ten employees - at the time for a sum of one billion dollars being an example of this.

Article 9: processing of sensitive data

The protection of sensitive data under the Regulation suffers from the following loopholes:

- Member States remain entitled to prohibit certain processing of sensitive personal data, even with the data subjects' consent (Art. 9(2)(a)). This runs counter to the harmonization intended by the Regulation and will inevitably lead to some processing being allowed in some Member States, while being prohibited in others, which is out of line with the broad consensus on consistency.

- Member States are obliged to provide (undefined) "adequate safeguards" in relation to the processing of sensitive data under employment law (Art. 9(2)(b)), as well as in relation to processing of criminal data. Furthermore they must provide (also undefined) "suitable measures" to safeguard data subjects' legitimate interests in relation to the processing of such data when "necessary for the performance of a task carried out in the public interest" (Art. 9(2)(g)). Here again, the risk is created of a lack of harmonisation which, in turn, will lead to forum shopping and a "race to the bottom" in relation to the elimination of data protection standards and safeguards for the protection of the right to privacy.

- The list of sensitive data under the Directive and the Regulation should be identical; beliefs should include philosophical beliefs; criminal convictions as well as offences must both be treated as sensitive data.

Article 20: measures based on profiling

What is profiling exactly and why is it problematic?

Data controllers can create profiles of data subjects by collecting personal data about them. Such

profiles and 'categories' of data subjects are being created in order to 'map' a person and to evaluate as well as analyze and predict (future) behavior. When more data become available, the profile becomes more precise and, consequently, becomes more valuable. The creation of profiles relies on increasingly complex algorithms, dynamically corrected and improved. The ever-increasing generation, capture and matching of personal information as well as information about objects that relate to individuals, such as cars, mobile phones, IP addresses and RFID chips, obtained in very different contexts, and of widely varying quality, create a new data environment that facilitates the ever-wider use of profiles for commercial as well non-commercial purposes. Profiles can be used for many different purposes, from marketing through the screening of job applicants, to credit-referencing and "-scoring", to law enforcement and the fight against terrorism. Online profiling, based on IP addresses and other online identifiers such as cookies, create profiles of internet users based on which they can be identified or singled out in the online environment. On the basis of their online profile, data subjects can be confronted with special offers, while other content may be withheld or prioritized differently.

Generally speaking, EDRi recognizes three main problems in relation to profiling of data subjects:

- Profiles can get it wrong, particularly when assessing uncommon characteristics. Where a profile is used as the basis for a fully automated decision, there is a risk that this decision is made on the basis of data that statistically apply to this person but that nonetheless give a wrongful impression of this person's behavior, health, preferences or reliability.

- Profiles can be hard or impossible to verify. Profiles are based on complex and dynamic algorithms that evolve constantly and that are hard to explain to data subjects. Often, these algorithms qualify as commercial secrets and will not be easily provided to data subjects. This non-transparency undermines trust in data processing and may lead to loss or trust in especially online services. There is a serious risk of unreliable and (in effect) discriminatory profiles being widely used, in matters of real importance to individuals and groups, without the required checks and balances to counter these defects.

- Profiles are likely to perpetuate and reinforce societal inequality and discrimination against racial, ethnic, religious or other minorities; this risk grows dramatically with the massive, almost explosive growth in data we are witnessing today. Continuous close scrutiny of the outcomes of decisions based on profiles, and of the underlying algorithms, is essential if these effects are to be avoided. Profiling creates an inherent risk of discrimination (e.g. in the context of access to goods and services) or other forms of unfair treatment, in particular increased surveillance if it is performed by public entities either directly or using data collected and processed by private companies.

What are the rules for profiling and what amendments are necessary?

Article 20 contains rules with respect to profiling. It states that every person has the right not to be subjected to measures that produces legal effects if these measures are solely based on automated processing. In order to build profiles of data subjects as described above, personal data is being collected and categorized. Both the collection and categorization can take place on one out of six legal grounds (article 6(1)), including the legitimate interest of the data controller. Sadly, the right not to be subjected to automated decisions is being diluted in article 20(2) through to article 20(4), resulting in too few safeguards against the negative effects of profiling on data subjects' privacy and other rights. EDRi proposes the following changes in order to protect data subjects from unwanted consequences of profiling.

- Article 20(1) should state explicitly that it applies to all kinds of profiling, both online and

offline. It is clear that the online environment allows for the creation of profiles of data subjects based on their behavior, through cookies, device fingerprinting or other means of gathering of user data.

– In order to regulate online profiling activities, it is necessary to recognise that online identifiers are personal data. Contrary to the initial draft and the interservice version, recital 24 currently states that online identifiers do not *necessarily* have to be considered personal data. This creates uncertainty as well as a legal loophole because it means that profiling online can take place based on these so-called identifiers, without the guarantee that the Regulation applies. EDRi therefore proposes the deletion of this recital, replacing it with the recital originally included in the interservice version, which stated that the Regulation will apply to online identifiers because these are associated with individuals and because online identifiers leave traces which can be used to create profiles of the individuals and identify them or single them out.

– Article 20(2)(a) must include the right for data subjects to be provided with meaningful information about the logic used in the profiling as part of the information duty applicable to data controllers, and, if human intervention has been obtained, the right to an explanation of the decision reached after such intervention. Also, data controllers must be accountable to DPAs in case there is a need for a DPA to assess whether profiling was lawful or not. They must therefore document the results of profiling and be able to demonstrate that profiling does not lead to discrimination. This will help make profiling more transparent and prevent discriminatory practices.

– Where Union or Member State law provides for 'suitable measures', as referred to in article 20(2)(b), such measures must specifically contain protection against discrimination as a result of automated decisions (profiling). This requirement also applies to the 'suitable safeguards' that must exist in the case where data subjects give their informed consent to the profiling.

– Use of sensitive personal data: in the private sector, profiling may never be based on or include sensitive personal data. In the public sector, profiling shall only involve use of sensitive personal data when these data are manifestly relevant, necessary and proportionate to the purposes of the legitimate public interest pursued, and even then should never be based solely or predominantly on those special categories of personal data.

– The Commission must adopt delegated acts for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subjects' legitimate interests referred to in paragraph 2 within six months of entry in to force and after consultation of the Data Protection Board on these proposals.