EXCEPTIONS (ARTICLES 2, 3, 10, 21, 80, 85)

Introduction

EDRi welcomes the fact that the Regulation applies to the processing of personal data in general. However, a number of significant and very broad exceptions provided for in the draft Regulation, if maintained in their current shape, will limit the application of this new legal framework and create new gaps in the protection of personal data. In order to foster uniform application of the new data protection regulation, the scope and number of these exceptions should be limited.

This paper outlines the most controversial exceptions together with their possible impact on the European standard of data protection and the reasons for limiting or removing these provisions.

Material scope: public security exception (Article 2)

According to Article 2 of the draft Regulation, the new data protection regime will not apply to the processing of personal data in the course of any activity concerning national security. The Council of the EU in its revised proposal would like to go even further, by adding the following additional grounds for limiting the applicability of the Regulation: defence, state security (including the economic well-being of the state when the processing operation relates to State security matters).

It seems that these general clauses are broad and flexible enough to contain not only activities that involve data processing by public entities in the context of national security but also data processing performed by private entities if commissioned by the state to carry out activities broadly related to public security, state security, defence or economic well-being of the state. In this context Article 2 might be used to limit the applicability of data subjects' rights not only with regard to public but also private entities. This concern should be addressed. In EDRi's opinion "national security" exception is broad enough to cover various instances of confidential data processing by state authorities and no other general clauses should be added in this article.

Material scope: maintaining separate legal regimes (Article 2)

Article 2 provides that the new Regulation will not apply to data processing: (i) by the European Union institutions, bodies, offices and agencies; (ii) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union; (iii) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. These exceptions implicate the continuation of separate data protection regimes for different areas. Except for the first exception, which is outside the scope of Union law, there is no convincing reason for maintaining separate legal regimes. All processing falling in any way under Union law should be covered by the Regulation, although in specific contexts, restrictions might be appropriate.

Material scope: personal or household activity (Article 2)

European Digital Rights
Rue Belliard 20, B-1040 Brussels
Tel:+32 (0) 2 274 25 70
E-Mail: brussels@edri.org, http://www.edri.org

Article 2 provides that the new Regulation will not apply to data processing "by a natural person without any gainful interest in the course of its own exclusively personal or household activity". The same exception is contained in the Data Protection Directive and, therefore, well established in the European data protection jurisprudence. On the basis of this jurisprudence it is clear that the definition of "exclusively personal or household activity" becomes more and more problematic in the world, where access to digital technologies that enable massive data processing is so common. In particular, this challenge is posed by the use of social networking services that enable processing of vast amounts of personal data and making this data accessible for literally unlimited number of users. In these circumstances it seems that maintaining equally broad exception for personal or household activity in the new Regulation will pose an increasing danger for data protection as there will be no legal instrument to defend data protection standards versus natural persons in their online activity.

In the context of the aforementioned challenges, EDRi welcomed a limitation of the exception for personal or household activity, namely providing that it applies only as long as data is not made available outside the immediate circle of such personal or household activity. This limitation was included in the inter-service draft circulated by the European Commission but was removed in the course of further legislative works. In EDRi's opinion this limitation should be re-introduced.

Material scope: relationship with e-Commerce Directive

According to Article 2(3), the new Regulation "shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive". While EDRi welcomes the concept of ensuring that the level of legal protection for intermediaries as provided in the e-Commerce Directive is maintained, in our opinion the relationship between these two legal acts should be further clarified. It is often the case that data protection standards are infringed not only by reckless or intentional behaviour of a given user (sharing personal data of other individuals) but also by the intermediary, who designed the service in the breach of respective standards. There is a variety of scenarios, where liability for the breach of data protection regulations may be shared, which will pose a serious challenge for jurisprudence.

Territorial scope: interpretative doubts (Article 3)

According to Article 3(1) of the draft Regulation, as far as its territorial scope is concerned, it will apply to the processing of data "in the context of the activities of an establishment of a controller or a processor in the Union". This phrase has been maintained from the current drafting of the Data Protection Directive. It should be noted that, on the basis of existing jurisprudence, that the very concept of data processing "in the context of the activities" posed serious interpretative difficulties in the course of implementing the Data Protection Directive. Therefore Article 29 Working Party and other authorities suggested that this phrase should be clarified. EDRi supports this recommendation in order to avoid potential disputes when data processing, in particular in on-line environment, is carried out "in the context of the activities of an establishment" and when not. EDRi feels that the established rules for the applicable law on for cross border sales of goods (as provided by for example the United Nations Convention on Contracts for the International Sale of Goods) provide a possible template for the rules to establish the territorial scope for the

Regulation.

Another potential interpretative challenge may be posed by Article 3(2), which provides that the new Regulation will apply to the processing of personal data if the processing activities are related to the offering of goods or services. In on-line environment vast majority of services is offered "for free" in the sense that service providers have other sources of revenue than users' fees (e.g. advertisement). Having that in mind it is very likely that the main question to be asked by the judges and Data Protection Authorities while applying Article 3(2) in practice will be whether it only refers to the offering of goods and services in return for a payment or other form of reciprocation. If the current drafting is maintained it will remain open for diverging interpretations to what extent commercial activity with no money flows between the service provider and the user or services delivered not-for-profit are covered by Article 3(2). In this context, EDRi would welcome adding provision stating that the Regulation would apply "irrespective of whether a payment of the data subject is required".

Processing not allowing identification (Article 10)

Article 10 of the draft Regulation refers to the situation when "data processed by a controller do not permit the controller to identify a natural person" and states that in this case "the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation". While EDRi agrees with the legal concept behind this provision, which constitutes a valid application of the principle of data minimisation, we see a serious challenge in determining when "data processed by a controller do not permit the controller to identify a natural person". The same interpretative doubts are posed by recital 23 of the draft Regulation, which provides that the principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

In EDRi's opinion the new Regulation should account for the challenge of achieving true anonymisation of data in the context of all available identification techniques and the prevalence of databases that enable crosschecks and re-identification of seemingly anonymous data. Therefore, in order to avoid interpretative doubts and potential abuses, additional provisions should be added, determining a number of conditions that need to be met for data to be treated as truly anonymised.

Restrictions (Article 21)

Article 21 provides for a number of general clauses such as "public security", "prevention, investigation, detection and prosecution of criminal offences", "the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions", "other public interests" or "monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority", which can be called upon by both each Member State and the European Union in order to restrict the scope of obligations and rights, which stem from general principles relating to personal data processing.

EDRi welcomes the fact that this possibility is limited by the requirement of proving that such a restriction "constitutes a necessary and proportionate measure in a democratic society". Nevertheless we find the catalogue of potential grounds for restricting the scope of rights of data subjects and respective obligations of data controllers extremely broad and unjustified, especially

in the context of general exceptions discussed above with regard to Article 2. The catalogue of permissible reasons for restrictions should be shorter. Similarly, the safeguards to be provided in acts restricting these rights should be strengthened, so that when Member States adopt such acts in accordance with their own constitutional requirements, it is ensured that the fundamental rights of data subjects are not unduly restricted.

Processing of personal data and freedom of expression: national exceptions (Article 80)

According to Article 80 each Member State shall provide for exemptions or derogations from the key provisions of the new Regulation (i.e. on the general data protection principles, on the rights of the data subject, on controller and processor, on the transfer of personal data to third countries and international organisations, on the independent supervisory authorities and on cooperation and consistency) for the sake of protecting freedom of expression (e.g. the processing of personal data carried out solely for journalistic purposes, for the purpose of artistic or literary expression). While EDRi welcomes this acknowledgement of the importance of balancing the right to privacy or data protection and the freedom of expression, the scope and possible implications of Article 80 pose serious concerns.

In particular, EDRi is concerned that due to such a wide scope for national restrictions and exemptions significant divergences in data protection regime applied in each of the Member States will be maintained, thus obstructing the main goal behind moving from the Data Protection Directive to the new Regulation.

In order to take account for the wider use of the Internet and its ability to support freedom of expression through citizen journalism, the restriction to (professional) journalistic purposes of this derogation should be removed. Furthermore, we believe that, both for legal and societal reasons, derogations must be "necessary". Such a limitation would help increase the possibility of a harmonised approach across Europe.

Churches and religious associations: exemption from the supervision of national DPAs (Article 85)

Article 85(1) provides that if churches and religious associations or communities apply, at the time of entry into force of the new Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, such rules may continue to apply, provided that they are brought in line with the provisions of this Regulation. According to Article 85(2) such churches and religious associations are also entitled to establish their own, independent authority in accordance with the provisions relating to national Data Protection Authorities. In EDRi's opinion these provisions will create a very serious exemption, thus limiting supervisory and executive powers of national Data Protection Authorities.

While it can be accepted that churches and religious associations apply their own rules with regard to the processing of personal data as long as these rules fulfil the standards determined in the new Regulation, it is difficult to justify why the practical application of these rules should be supervised by another authority. This situation may lead to the development of diverging lines of jurisprudence and different data protection standards applying to the same or very similar situations depending on quite irrelevant circumstances, which is belonging to a given church or religious association.

Therefore EDRi recommends that Article 85(2) be deleted and replaced with a provision making it clear that the application of comprehensive data protection rules developed by a church or religious association will be supervised and executed by the national Data Protection Authority. Moreover, any exceptions for churches and religious associations should be limited to personal data about their own members.