FUNDACJA PANOPTYKON

REFORM OF THE EUROPEAN PERSONAL DATA PROTECTION LAW

Executive summary

In connection with the intensification of legislative works in the European Parliament and the Council of the European Union, we hereby present a summary of the recommendations and observations of Panoptykon Foundation, regarding the draft General Data Protection Regulation[1]. The document contains an assessment of the draft regulation in the version prepared by the European Commission and the direction of changes visible in the works in the Council. In our opinion, the draft of the European Commission should be treated as a reference point for further legislative works. Amendments tabled by the EU Council and the European Parliament should not lead to a decrease in the proposed level of personal data protection.

From the perspective of citizens, the most important proposals included in the project are:

- a broad, yet still flexible definition of personal data and a data subject, taking into account the development of technology facilitating the combining of data and (re-) identification (Art. 4.1);
- a precise definition and a high standard of consent to personal data processing, in particular the requirement of obtaining "explicit" consent (Art. 4.8, Art. 6.1a and Art. 7);
- the requirement of ensuring maximum protection of privacy by default (Art. 23).

The draft the European Commission has also weak points, which – under the influence of extensive legal interpretation or amendments leading to a further lowering of the standards of personal data protection – may undermine the whole purpose of this legal regulation:

- very broad exceptions from limitations provided for measures based on profiling (Art. 20);
- the clause of "legitimate interest of the data controller" – imprecise and vulnerable to misuse – as one of the equally valid grounds for personal data processing (Art. 6.1f).

Assessment of the most important proposals contained in the draft Data Protection Regulation

If research findings are true, more and more people admit that they do not feel safe in the circumstances of a constant flow of data beyond their control and that in this scope they do not trust the companies whose services they are using. Citizens display a greater need to have control over personal data, and the present model of commercialization of information is not widely accepted[2].

We fully agree with the view of EU Justice Commissioner Viviane Reding that it is high time that we adjusted the privacy protection standards to the challenges laid before us by the development of technology. Non-adjustment of many legal norms to the realities of the Internet, as well as a lack of a uniform privacy protection standard in the European Union make this one a very urgent task.

In our opinion, the draft regulation presented by commissioner Reding at the beginning of the previous year aims at strengthening the standards of personal data protection and their adjustment to the present market practices. Therefore, it should be treated **as a reference point for further legislative works**. Amendments proposed by the Council of the European Union and the European Parliament **by no means should lead to a decrease in the level of protection proposed by the European Commission**. Yet, at the same time, in several

[1] Draft regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012/0011 (COD), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:PL:PDF.

[2] [2] Eurobarometr, *Attitudes on Data Protection and Electronic Identity in the European Union,* June 2011, http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_fact_pl_en.pdf .

significant points the draft prepared by the European Commission requires strengthening or "tightening" so that the aims of the reform could be fully achieved.

Below we discuss and assess the most important proposals contained in the draft General Data Protection Regulation which either constitute a foundation of this legislative initiative, or pose a threat to this foundation.

(i) Definition of personal data and data subject

Relevant article of the draft: **Art. 4. 1.**

What the draft of the Commission provides for: The term "personal data" means each piece of information regarding a data subject, whereas the "data subject" – each person whom it is possible to identify indirectly or directly. This is a good, broad definition, although for the next 20 years even this one may prove insufficient. The definitions of personal data and a data subject are the foundations of the entire draft. The applicability of the new law depends on how broad they will be.

Direction of changes proposed by the Council: As a result of discussions held in the DAPIX working group, the definitions of personal data and a data subject have been combined. Such a solution does not seem transparent and makes it difficult to precisely build both definitions.

Recommendations of Panoptykon Foundation:

- Extending the definition of a data subject **by the criterion of singling out**.
- Preservation of the **criterion limiting** the definition of personal data: „by means reasonably likely to be used by the controller or by any other natural or legal person", proposed by the European Commission
- **Preservation of** both **separate** definitions – of a data subject and personal data.

Justification:

More and more frequently, especially on the Internet, it is not necessary anymore to identify a person in order to be able to **significantly interfere with his or her privacy** – it is enough to be able to „single him or her out" from the group of the remaining users, e.g. through a unique profile generated on the basis of a digital trace, even if it is not combined with any permanent or temporary identifier. We are dealing with such a situation every time the profiling and influencing of user's decisions is based on the information included in a cookie file or obtained on the basis of other tracking techniques. On that basis one may successfully match e.g. an advertisement playing on emotions to a child sensitive to such emotions or an offer to purchase slimming products to a teenage girl suffering from anorexia.

The law should take into account the fact that inevitably there will be emerging **new technical measures enabling identification** of people, hence items of information which due to that criterion could not have been regarded as personal data several years ago, will be able to be given such a status **in the near future**. Easiness of combining data and re-identification of individuals on that basis is confirmed by scientific research[3].

Along with the emergence of new possibilities of identification of individuals, the scope of applicability of standards for personal data protection should also increase. The definition proposed by the European Commission ensures such flexibility, whilst containing reasonable limitation in the form of the criterion of probability that the measures enabling identification will be used by the data controller or another person (natural or legal).

[3] According to the research conducted by Professor Latanya Sweeney (Harvard University), in order to identify 87,5 % of Americans it is enough for an entity to know only the zip code of an individual, his or her gender and date of birth. Latanya Sweeney, *Uniqueness of Simple Demographics in the U.S. Population* (Laboratory for Int'l Data Privacy, Working Paper LIDAP-WP4, 2000).

A similar position was taken by Art. 29 Working Party [4].

(ii) Pseudonymous data

Relevant article of the regulation: the draft of the Commission does not contain any proposals regarding pseudonymous data.

Direction of changes proposed by the Council: During the works of DAPIX working party, the definition of pseudonymous data was included in the draft regulation. It can be found in Art. 4.2a.

Recommendations of Panoptykon Foundation:

- **We do not object to** the very introduction to the draft regulation of the definition of pseudonymous data. We demand however that it should be made more precise in order to avoid interpretational doubts.
- We call for an introduction of provisions guaranteeing that additional information enabling identification will be stored not only in **a separate set**, but also secured using **independent organizational and technical means**.
- We categorically **oppose to amendments aimed at excluding pseudonymous data from the regime of personal data protection** or lowering the standard of protection in relation to this category of personal data.
- However, we allow for exclusions from certain obligations towards a data subject, if it is not possible to meet them without a full and direct identification.

Justification:

Adding the definition of pseudonymous, or pseudonymised data may not be treated as a „foothold" for creating separate principles for the processing of this type of data. **There may be no doubts that pseudonymous data fall within the definition of personal data, as they simply are data enabling indirect identification**. This is confirmed not only by an analysis conducted by authorities in the domain of data protection (see below), but also numerous examples showing how easily one may rebuild a connection between pseudonymised data, and data directly identifying a given individual.

For instance, in 2006 the American website Netflix (an on-line movie rental site) made public the information concerning which films are watched and how they are rated by over 500 thousand of its users. All the information enabling direct identification of particular persons (e.g. a user's name) was removed from the study, while at the same time numbers were distributed to particular individuals (anonymisation). Hence it was known, that, for instance, user 1345 rated a certain film with 5 stars. Scientists from the University of Texas, Arvind Narayanan and Vital Shmatikov have proven that anyone from outside, having so little information as an individual number, may in 84% cases make an errorless identification of particular users of that site[5].

Excluding pseudonymous data from the regime of personal data protection **poses a risk for the integrity of the entire system**. Such a view is also expressed in the official stances of the European Data Protection Supervisor[6] and Art. 29 Working Party[7]. The authors of the new regulation should seek to create a **coherent**

[4] Opinion of Art. 29 Data Protection Working Party no. 4/2007 on the concept of personal data of 20 June 2007, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.
[5] Arvind Narayanan, Vitaly Shmatikov, How to Break the Anonymity of the Netflix Prize Dataset, ARVIX, 2006, http://arxiv.org/abs/cs/0610105v1.
[6] Additional comments of the European Data Protection Supervisor on the data protection reform package of 15 March 2013, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2013/13-03-15_Comments_dp_package_EN.pdf.

system of legal protection, without broad exclusions and separate regimes, which, as a principle, cause difficulties in interpretation and leave room for misuse.

(iii) Definition and conditions for granting consent for data processing

Relevant articles of the draft regulation: **Art. 4 ,8, Art. 6.1 a and Art. 7**

What the draft of the Commission provides for: One out of six grounds for processing personal data is a consent granted by the data subject. According to the draft proposed by commissioner Reding, such a consent must be explicit – it cannot be implied from our behaviour, as in practice it would leave room for obvious misuse. On the other hand, the burden of proving that consent has been given by the data subject shall be carried by the data controller.

Direction of changes proposed by the Council: In the latest proposals, the requirement of obtaining explicit consent is replaced by a less precise criterion of "unambiguousness". This is a return to a lower standard of legal protection provided for by the currently binding Directive 95/46/EC.

Recommendations of Panoptykon Foundation:

- **We fully accept the definition of consent proposed by the European Commission**, in particular, the introduction of the requirement to obtain express consent and the emphasis on its voluntary nature.
- **We object to all or any amendments which would lower the standard required for deeming a declaration of will of the data subject to be a consent** for personal data processing, in particular, resignation from the requirement to obtain express consent for personal data processing and from a limitation in accordance with which **consent obtained in a situation of a significant inequality of the parties may not be deemed voluntary**.
- As this is a crucial, independent basis for personal data protection, consent in any circumstances must be explicit, voluntary, referring in detail to a specific purpose and scope of data processing and based on reliable information.
- In practice, data controller should not have the possibility to process data basing on "pre-ticked boxes", or to presume that consent has been granted on the basis of other behaviours of data subjects.

Justification:

The criticism of the definition of consent proposed by the European Commission expressed by certain business environments disregards a fundamental fact that **consent of the data subject constitutes one of the six independent grounds for personal data processing**. This particular basis is aimed at safeguarding the information autonomy of the data subject in a situation, where the possibility to process data depends exactly on his or her decision. One shall bear in mind that this is an extraordinary situation, occurring when the need to process data does not arise out of contractual or legal provisions.

In the case of online services, a common practice is data processing based on **implied consent** (e.g. due to the very fact of entering a website or using a service). However, research conducted both in Europe and the United States has shown that such a presumption is not based on the actual level of awareness of users[8].

The proposals tabled in the Council return to the conceptual network of the currently binding Data Protection Directive (see article 7 point (a)). The practice of its application has shown that the criterion of

[7] Additional opinion of Art. 29 Data Protection Working Party, no. 08/2012 on the data protection reform proposals of 5 October 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf.

[8] Compare, e.g.. Big Brother Watch, „Nine in ten people haven't read Google's new privacy policy", http://www.bigbrotherwatch.org.uk/home/2012/02/ten-people-havent-read-googles.html; Rebecca Smithers, "Terms and conditions: not reading the small print can mean big problems", The Guardian, http://www.guardian.co.uk/money/2011/may/11/terms-conditions-small-print-big-problems.

"unambiguousness" is vulnerable to extensive interpretation. In effect, under the current regime application of the provisions defining the notion of consent is neither coherent nor consistent. Basing on the concept of an "unambiguous" consent, such practices have developed as placing the consent clause in general terms and conditions and regulations or implying consent from different behaviours of the user, only providing that the user has been informed about the consequences (e.g. of entering a website or using the services of a web portal). Upholding this concept in the new regulation will be tantamount to accepting the practices which by no means guarantee the information autonomy of data subjects.

In accordance with the opinion of Art. 29 Working Party, including in the regulation a safeguard that consent must be explicit is essential for ensuring data subjects the possibility to exercise their rights. Since it is one of the independent prerequisites for processing personal data, the regulation must guarantee an appropriate standard for a declaration of will of so profound consequences. The European Data Protection Supervisor also agrees with this opinion[9].

The criterion of voluntariness of consent means that **the user must have the possibility of an actual choice as to whether or not he or she wishes to grant consent for data processing**. Such a possibility does not exist in a situation of a significant inequality between the data controller and the data subject, e.g. in the relationship of the employer with employees or in the conditions of a monopoly or market domination (when the data controller has a monopolistic position on the market and offers services which are not available from anyone else).

(iv) Limitations for measures applied on the basis of profiling

Relevant article of the draft regulation: **Art. 20**

What the Commission draft provides for: The draft prepared by commissioner Reding provides for a **regulation of measures (e.g. decisions) based on profiling in relation to which it formulates several limitations**. For instance, it grants a person subjected to such measures a right to receive "human intervention", if he or she does not agree to the decision reached. **The proposed regulation is of a very gentle nature: it does not mention any ban on profiling, and the stipulated exclusions have a broad scope**.

Direction of changes proposed by the Council: There emerged a proposal to add the definition of profiling to the draft regulation (Art. 4.12a). In relation to measures based on profiling, it is proposed to condition the scope of application of the proposed provisions on what effect a given measure based on profiling has and whether or not it is an "adverse" effect ("measures adversely affecting data subject").

Recommendations of Panoptykon Foundation:

- Maintaining **uniform rules regarding measures based on profiling regardless of how they affect** the data subject. In our opinion, conditioning the scope of a legal regulation on such a subjective criterion undermines the very purpose of that regulation.
- **Making** the definition of profiling **more precise** and **extending** it by processes which do not rely only on **automatic data processing**.

[9] "(...) the EDPS stresses that the concept of explicit consent as currently defined in the Commission proposal (in particular Articles 4(8), 6(1)(a) and 7) should be maintained. It provides for some flexibility as to its manner of expression (by a statement or a clear affirmative action) and builds on the requirement of 'unambiguous' consent which constitutes an essential element of the overall balance of data protection since 1995. EU data protection authorities have consistently interpreted the requirement of Article 7(a) of Directive 95/46/EC, in relation to Article 2(h), that the consent be 'unambiguous' as meaning that such consent needed to be 'explicit'10 (so that, for instance, a lack of action or silence cannot be considered as unambiguous). Consequently, the EDPS recommends that amendments such as ITRE AM 83, IMCO AM 63, and proposed LIBE AM 757, 758, 760, 764-766 etc. be rejected". Additional comments of the European Data Protection Supervisor on a data protection reform package of 15 March 2013, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2013/13-03-15_Comments_dp_package_EN.pdf.

- **Limiting the possibility to use sensitive data** in the process of profiling in order to diminish the risk of discrimination.
- **Safeguarding to data subjects the right to information** on whether or not they are subjected to profiling, what logic stands behind the applied algorithm and to what categories their data have been qualified, as well as the right to explain the final decision. These safeguards will help limit the lack of transparency which undermines trust in data processing entities, especially in the context of online services.

Justification:

Profiling, that is collecting and automatic processing of information about us in order to build certain assumptions on our personality and future behaviours, involves many risks. The most important one is a **risk of discrimination, exclusion and solidification of social stereotypes**.

Profiling is based on statistical correlations, thus in principle carries a significant margin of error. From the perspective of the data processing entity, this margin may be minor, nevertheless, from the perspective of a person falling within its boundaries, such an error is of essential importance – **it may lead to racial discrimination, exclusion from access to a significant service, discrimination in terms of price, breach of privacy and other negative effects**[10].

From the point of view of the data subject **what is important is not only the creation of an individual profile, but the very qualification of him or her to a specified group**. From the perspective of information autonomy of the data subject it is important that the data controller knows for certain that a given data subject belongs to a specific category (e.g. individuals who are homosexual, overweight, divorced, etc.) and is capable of using this knowledge. Therefore, apart from the criterion of identifiability, **we need to introduce the criterion of singling out, at least in the provisions regarding profiling**.

Created profiles may be difficult or even impossible to be verified, as they are based on complex and dynamic algorithms. Algorithms used in this process are frequently qualified as a trade secret, in the light of which individuals subjected to profiling have no access to the information which concerns them. In this context, **safeguards increasing transparency of measures based on profiling** from the perspective of the data subject are of great importance.

Due to those inherent risks, **tight regulation is necessary which – not banning such practices – will ensure appropriate safeguards in each instance of applying measures based on profiling**. Therefore, we strongly oppose to the conditioning of the scope of the proposed regulation on what effects are exerted by a measure based on profiling ("significant" or "adverse"). Such a structure conditions data protection standards on the self-evaluation and good faith of data controllers, creating a significant gap in the regulation.

Similar reservations and remarks have also been made by Art. 29 Working Party in its opinion to the draft regulation[11].

(v) Privacy by default – maximum privacy protection

Relevant article of the draft regulation: **Art. 23**

[10] E.g.: Dominic Basulto, "Is social profiling discrimination?", The Washington Post, http://www.washingtonpost.com/blogs/innovations/post/is-social-profiling-the-new-racism/2012/05/03/gIQAXQQDzT_blog.html; Herb Weisbaum, "Google ads may be racially biased, professor says", NBC News, http://www.nbcnews.com/business/google-ads-may-be-racially-biased-professor-says-1C8369538; Report of the European Union Agency for Fundamental Rights , "Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide", http://fra.europa.eu/sites/default/files/fra_uploads/1133-Guide-ethnic-profiling_EN.pdf; Jakub Mikians, László Gyarmati, Vijay Erramilli, Nikolaos Laoutaris, "Detecting price and search discrimination on the Internet, HotNets-XI Proceedings of the 11th ACM Workshop on Hot Topics in Networks", http://www.tid.es/es/Lists/Scientific_Publications/Attachments/251/hotnets2012_pd_cr.pdf.

[11] Opinion of Art. 29 Data Protection Working Party, no. 01/2012 on the data protection reform package of 23 March 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf.

What the draft of the Commission provides for: Commissioner Reding proposed **a change of the paradigm in the relationship client vs. service provider – from "tracking by default" into "privacy by default**". In accordance with this model, as early as upon the moment when we start to use a given site or service, we should have the maximum protection of privacy ensured. The draft regulation imposes on the data controller an obligation to ensure that only these data will be processed by default which are essential for the implementation of a specific, pre-designed purpose (both when it comes to the quantity of data, and the time of their processing). In particular, the data controller should ensure that by default personal data are not made available to an unlimited number of persons.

Direction of changes proposed by the Council: The proposals being discussed provide for a limitation of the obligation to ensure that by default personal data are not made available to an unlimited number of persons, through adding the phrase "without human intervention". It is also proposed to replace the reference to "state of art" in the context of implementation of appropriate technological means by the data controller with a reference to "available technology", without defining that notion.

Recommendations of Panoptykon Foundation:

- The Commission's proposal is heading to a good direction and should be preserved – in particular as regards the express obligation to ensure that by default personal data will not be made available to an unlimited number of persons.
- At the same time we propose to **further specify the definition** of privacy by default and to make it uniform with the definition of privacy by design **through a reference to technical and organizational means**, which should be provided by the data controller in order to fulfill this obligation.

Justification:

The principle of privacy by default leads to the protection of data subjects, also in a situation of not understanding or a lack of control over the manner in which their data are processed, especially in the context of technology. At the core of this principle is an assumption that the functions of a given product or a service, which potentially may pose a threat to privacy, are at the outset limited to what is absolutely necessary. In this model, a decision on extending the possibility to process data is to be taken exclusively by the data subject[12].

Thereby, the principle of privacy by default protects personal data against exploitation by the very service provider. At the same time, **it is not about a ban on data processing, but about respecting fundamental principles, such as proportionality and adequacy of what is collected about us to what is offered to us**.

The risk of making data available to an unlimited number of recipients and irreversible consequences connected therewith exist not only in the case of automatic data processing (i.e. "without human intervention"). Such a disclosure may occur e.g. as a result of a decision of an employee authorized to process data, or of the data controller. Therefore, Art. 23 should allow for that only in the case of an informed consent of the data subject himself or herself.

(vi) Legitimate interest of the data controller

Relevant article of the regulation: **Art. 6.1 f**

What the draft of the Commission provides for: The draft regulation provides for six grounds for processing personal data, among them, the so-called legitimate interest of the controller. That ground allows for personal data processing without consent of the data subject, in the case when in the opinion of the controller his legitimate interest prevails over the interest or fundamental rights of the data subject.

[12] Additional comments of the European Data Protection Supervisor on the data protection reform package of 15 March 2013, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2013/13-03-15_Comments_dp_package_EN.pdf.

Direction of changes proposed by the Council: Among the latest proposals, there is a possibility to extend the notion of legitimate interest of the data controller by "third parties", i.e. other controllers to whom data are made available.

Recommendations of Panoptykon Foundation:

- **We propose to better define** the notion of legitimate interest of the data controller and to secure this basis for data processing by **additional safeguards**.
- In particular, we propose to introduce a principle that this legal basis can be used only when data processing based on the remaining legal grounds turned out impossible or excessively difficult and only when it is justified by the contractual relation or "reasonable expectations" of the data subject.
- We demand that the proposal of the European Commission which **limits the possibility to use this legal ground to the original data controller** be preserved**.** However, we allow for an exclusion in a situation, when the contractual relation or "reasonable expectations" of the data subject justify the processing of data by "third parties".

Justification:

The notion of the legitimate interest of the data controller is **unclear, involves arbitrariness** and leaves **vast room for interpretation**. Art. 6.1f assumes **good faith of the controller** who alone is to decide whether or not data can be processed (without consent of the individual to whom such data refer), while he **should not be the judge in his own case**.

The application of this prerequisite results in a situation where **data processing becomes non-transparent** from the perspective of individuals to whom such data refer, leading to the **erosion of trust** between the data subject and data controller[13].

Moreover, interpretation of this clause may vary in particular member states, thereby undermining the very purpose of harmonization and introducing uncertainty as to the scope and legality of certain forms of data processing.

The observations of the existing market practices force one to assume that in the case when mass data processing is at stake, **the interest of the data controller will always prevail over that of the users**. In the course of applying Directive 95/46/EC the "legitimate interest clause" became a standard justification for data processing, exceeding beyond what is necessary for the performance of an agreement or obligations arising out of the provisions of law.

An example of such a practice (which has been criticized by European personal data protection supervisors) may be a recent **change of privacy policy of Google**, involving integration of data processed in connection with various services rendered by this company. Also **expanded ecosystems of direct marketing operate on the basis of this legal ground**, where persons whose data are processed and combined into extended profiles have no control over that process, and often even no knowledge of all the entities engaged therein.

A structure enabling the application of this legal basis by third parties is considered by us as particularly unwanted and dangerous. Such an approach essentially **undermines the principle of information autonomy as well as purpose limitation of data processing**. A data subject would simply be deprived of actual control over by whom, in what scope and for what purpose his or her data are processed by further controllers.

[13] Examples of misuse and a very broad application of legitimate interest are numerous: (a) Google is processing a majority of user data basing on legitimate interest. Privacy policy of this company indicates that it collects a wide range of data on an individual. The controversial decision of the corporation to create one privacy policy for all of its sites has led to actions being initiated against Google by personal data protection authorities in six member countries of the European Union (http://www.rp.pl/artykul/995952.html); (b) Linkedin: once installed on mobile devices, purported to give access to the meetings calendar, the application started collecting all data stored in the device. The company pointed out to legitimate interest as a ground for such a state of affairs.

With respect to those risks**, the principle expressed in Article 6.1f should be formulated as narrowly as practicable**. Originally, that basis for data processing was as a matter of fact thought of as an exception and one shall return to this assumption.

(vii) Data transfers to third countries or international organizations

Relevant articles of the regulation: **Art. 40-45**

What the draft of the Commission provides for: The draft regulation provides for two basic situations in which it is possible to transfer data to third countries: the issuance by the European Commission of a decision confirming the appropriate level of data protection or the existence of the so-called appropriate safeguards. Unfortunately, there are numerous exceptions from those two principles, unfavourable from the point of view of data subjects.

Direction of changes proposed by the EU Council: The latest proposals discussed in the DAPIX group are aimed at depriving the Commission of the possibility to reach an independent decision on there being no appropriate level of data protection in a third country. The European Commission will only be able to revise an already issued favourable decision. It is also proposed to remove from Art. 42 the requirement to include a data protection safeguard in a legally binding instrument. As regards exemptions from Art. 44, the proposals of DAPIX group are aimed at making the notions of "legitimate interest" and "public interest" more detailed.

Recommendations of Panoptykon Foundation:

- The European Commission should have the possibility to issue a decision asserting both the relevant level of data protection and there being no appropriate level of data protection. It is also important to create a mechanism making it possible to revise an already reached decision. We also call for adding to this procedure an obligation to request the opinion of the European Council for Data Protection.
- We believe that safeguards being a basis for data transfers should be included in a binding legal instrument.
- We call for the introduction of at least a minimum safeguard protecting data controllers against the necessity to make personal data available to authorities of third countries which are not bound by appropriate international agreements with the EU and thereby cannot guarantee the proper standard of protection of data subjects' rights.
- We believe that exemptions set forth in Art. 44 should be significantly limited. We propose that it should be admissible to apply them only in the case of transfers of an incidental character. We also propose to erase from the catalogue of exemptions two prerequisites: legitimate interest of the data controller and public interest.

Justification:

Data transfers to third countries is a politically sensitive topic. The regulation seeks to reconcile two aims which may be in conflict: data protection and facilitating data transfers to third countries which may not ensure the appropriate level of their protection. As the controversies connected, say, for instance with *Safe Harbour* programme demonstrate, third countries not always ensure Europeans the proper standard of personal data protection. Therefore, European law should provide for stronger safeguards for respecting the minimum standards in that scope than those applied so far.

The possibility to issue a decision asserting a lack of the appropriate level of data protection constitutes a powerful tool in the hands of the Commission which may be employed to exert pressure on third countries. On the other hand, due to the political dimension of transferring personal data beyond the borders of the EU, the decision on acknowledging foreign legal safeguards as adequate should not be left for the assessment of the European Commission alone. Hence the proposal to include the obligatory assessment of the European Council for Data Protection.

The exemptions stipulated in Art. 44 from the rule, in accordance with which a decision is required confirming the appropriate level of data protection or the appropriate safeguards, constitute a very dangerous and incomprehensible gap in the European standard of personal data protection. In particular, this refers to the possibility to transfer data on the basis of the legitimate interest of the data controller or the prerequisite of public interest. It is difficult to logically justify why data transfers to a third state, which does **not** guarantee the appropriate level of personal data protection, would be admissible basing on the same premises which justify data processing in the framework of the EU (with very high legal safeguards). Therefore, we call for a limitation of the scope of application of art. 44 to the transfers which are not "massive, frequent or structural"[14]. Data controllers enticed by the possibility to rely on exemptions, may not want to provide appropriate safeguards for data protection.

In the light of reports on the scale of exploitation of personal data of European citizens by secret services of other states, particularly the USA, it also seems necessary to return to the original wording of art. 42, proposed by the Commission in December 2012. Data controllers should have the right to refuse to make data available to authorities of the states not being members of the EU, if an international agreement does not stipulate appropriate safeguards, and the obligation to notify European authorities on the fact of data having been made available. The introduction of such a provision will not solve the problem of conflict of laws, which the data controller will have to face (being at the same time obliged to apply a foreign law), but it will give the EU a better position in negotiations on international level and will increase the transparency of transfers.

FUNDACJA PANOPTYKON

[14] This view is expressed by Art. 29 Working Party - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf .