SDRUŽENÍ
PRO INTERNETOVOU
REKLAMU

Registered Office: Korunní 79/1171, 13000, Prague 3, Czech Republic
Telephone: +420 224 251 250 **E-mail:** info@spir.cz **Internet:** www.spir.cz
Bank Account: Raiffeisenbank **Acct. No.:** 375076001/5500 **Business ID:** 70108005 **Tax ID:** CZ70108005

Subject: SPIR Comments on the Draft of the Regulation on Protection of Individuals

Comments by the Association for Internet Advertising (hereinafter referred to only as SPIR), a professional association of legal entities, on the draft of the Regulation of the European Parliament and the Council on Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of These Data (general regulation on data protection).

The aim of the draft of the New *Regulation of the European Parliament and the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of These Data* (hereinafter referred to as "Draft Regulation" or "Regulation") according to the European Commission ("Commission") is especially to create a pan-European applicable framework for the protection of personal data and to contribute to greater consumer confidence when shopping online. The Regulation is also supposed to respond to new trends and an increased range of personal data gathering online.

From the perspective of entities providing information services on the internet in the Czech Republic, it must be said that the current arrangement under Directive No. 95/46/ES and its follow-up Act No. 101/2000 Coll., on Personal Data Protection, as amended, appears to be quite sufficient and does not need to be replaced by a new comprehensive arrangement. Changes that could perhaps be induced in connection with the development of new technologies and that lawmakers saw the need to regulate could be implemented in a sufficient manner through amendment to Directive No. 95/46/ES.

From a general perspective, the new legal treatment does not represent any new fortification of legal protection compared to the current status. On the contrary, the introduction of a whole series of new institutions will lead to an increase in legal uncertainty among businesses operating in the market without bringing an unambiguous improvement for data subjects. The new legislative regulation also represents — despite opposite proclamations in its explanatory Memorandum — a considerable increase in administrative burden for small and medium companies. These companies usually do not expand beyond the borders of their national states, so they will not benefit from a single pan-European regulation, but instead feel the weight of the newly established restrictions and increased administrative burden. The Draft Regulation will not in any way contribute to the development of business, especially of the small and medium type,

It should be noted that according to our preliminary calculations of costs related to the implementation of the restrictions imposed by the Draft Regulation, it seems likely that as a result of the Regulation costs for companies with more than 250 employees will increase by at least CZK 1.2 — 2.2 million annually.

Among the individual provisions of the Draft Regulation, we would like to point out these problematic points:

1. **Article 3, paragraph 2 —** *This provision expands the scope of the Regulation to entities not seated in the Union, if they monitor behavior of persons residing in the Union or offer to sell goods to them.*

Registered Office: Korunní 79/1171, 13000, Prague 3, Czech Republic
Telephone: +420 224 251 250 **E-mail:** info@spir.cz **Internet:** www.spir.cz
Bank Account: Raiffeisenbank **Acct. No.:** 375076001/5500 **Business ID:** 70108005 **Tax ID:** CZ70108005

Thus the provision remains solely on a proclamatory level, because the Union does not have the tools to enforce the observance of its laws beyond its territory. In internet business practice we increasingly more often observe that entities standing beyond the regulations of the Czech Republic or, by extension, of the entire Union, derive benefits from the often simpler and more benevolent legislation in their home states. Yet the internet environment by its very nature does not recognize borders and enables the addressing of users in one state from another state. The European lawmaker's notion of making regulations stricter for entities seated in the Union and attempting to restrict their foreign competitors by extending the effective range of domestic legislation to their activities is completely unrealistic, and thus significantly hampers economic competition between European entrepreneurs on the internet versus their global competitors. The European legislator should rather strive to ensure that the degree of legal regulation within the EU is limited to the necessary minimum that would still result in adequate protection of the rights of individuals.

2. **Article 4, paragraph 1 —** *Added to the definition of personal data as one of the elements enabling identification was an "electronic identifier," which is primarily directed at so called cookies. The definition does not specify whether the Regulation applies only to persons living or to deceased persons as well.* The interpretation of this provision is partly given in recitative 24, which however is not entirely compatible with the text of the definition provided in Article 4 paragraph 1. In interpreting the text of the definition given in Article 4, it seems as if the electronic identifier alone (cookies) was sufficient for identifying the subject of the data. In contrast, recitative 24 assumes – as it seems – that cookies alone do not necessarily have to be personal data. Cookies alone in fact do not identify a concrete individual, but only a concrete computer, regardless of how many people use that computer. To the controller, the cookie thus does not – without combining with other information – make it possible to identify the user (or several users) of some computer as a concrete person. In terms of the definition personal data, it will thus be a matter of dispute whether the interpretation arising from the text of Article 4 of the Regulation should take precedence, or from the text of point 24 of the recitative. **We believe that it is necessary to resolve this contradiction unambiguously before the adoption of the statutory text, and in such a way that cookies alone are not deemed capable of identifying the data subject. This is a crucial question for the whole application of the Regulation to internet business. If the legislature leaves this question unresolved, it will mean considerable uncertainty for entities active in the market in the first several years of Regulation application. As far as deceased persons are concerned, we believe that the Regulation should not apply to them.**
3. **Article 5, letter c)** directs that only the necessary minimum of information may be processed. The Regulation does not make any allowances for a situation when a greater than minimal quantity of information is processed with the informed consent of the data subject. Such a limitation of dispositional authority of the data subjects with regard to their own data, however, is totally unacceptable.

4. **Article 6, paragraph 1 —** *This article stipulates the cases when it is possible to process personal data under the law.* In our opinion, exceptions for freedom of expression are not sufficiently anchored here. In particular the construction of letter f) in effect means that the individual that crossed the permissible limits of freedom of expression could be punished, in additional to standard

Registered Office: Korunní 79/1171, 13000, Prague 3, Czech Republic
Telephone: +420 224 251 250 **E-mail:** info@spir.cz **Internet:** www.spir.cz
Bank Account: Raiffeisenbank **Acct. No.:** 375076001/5500 **Business ID:** 70108005 **Tax ID:** CZ70108005

forms of compensation (through lawsuits claiming protection of name and reputation), in the form of a fine under the Regulation. This will consequently lead to self-censorship and restriction of free political discussion. We therefore believe it is appropriate to remove questions related to freedom of expression from the Regulation entirely (see also commentary on Article 80), also given the context of the new UN resolution promoting freedom in the digital world as one of the basic human rights.

5. **Article 6, paragraph 4 —** *enables the processing of personal data even after the original purpose is gone.* This provision refers to such purposes only for cases listed in paragraph 1 under letters a) to e), and for unclear reasons omits the processing purpose under paragraph 1 letter f). We recommend that a reference to letter f) be added here as well. Similarly missing without reason is a reference to paragraph 2.
6. **Article 6, paragraph 5 —** *This paragraph authorizes the Commission to issue acts under delegated powers for the purpose of further limitation of conditions under which it is possible to process personal data, if it is "*necessary *for realizing the legitimate interests of the controller".* We believe that such an important question should not be removed from the competence of the European legislature and entrusted to a mere administrative body such as the Commission. We recommend that it be omitted.
7. **Article 7, paragraph 1 —** *transfers the burden of proof that the data subject gave consent to his being processed to the controller.* We believe that in some cases such transfer of the burden of proof would be inappropriate. This provision should be mitigated at least to such extent that the transfer of the burden of proof does not occur in cases when it was evident from the subject's behavior that their consent had been expressed.
8. **Article 7, paragraph 4 —** *According to this provision, the expression of consent does not provide a legal basis for the processing of data when a significant imbalance exists between the individual's standing and that of the controller.* This is particularly the case in the employee – employer relationship, according to the recital. But the given provision completely overlooks the fact that if there is an imbalance between the administrator and the individual, such a state of disequilibrium may manifest itself only in some aspects. For example, an employee gives their employer, who operates an internet store, consent to process personal data in connection with shopping at this store (which will not be related in any way with their employment). The clause should therefore be supplemented to state that the imbalance must be related to the concrete case of personal data processing to which consent is granted.
9. **Article 8 —** *the necessity to authorize the consent of a child under the age of 13 by a parent.* Paragraph 1 clearly states that the consent of a child under the age of 13 must be approved by a parent of the child. In practice, however, it is often not possible – especially on the internet – to find out whether the person granting consent is under the age of 13 or not. In this context, not even putting in a field for age helps, since the child may enter false information, and furthermore such a requirement would often lead to superfluous archiving of unnecessary data on age. In practical terms, it seems that it would be more appropriate to make an adjustment to Article 8 that would omit the obligation to get consent from parents, and the controller of data would be obligated to erase data which he reliably learns that it concerns a child under the age of 13 without parental consent for their processing having been granted.

Registered Office: Korunní 79/1171, 13000, Prague 3, Czech Republic
Telephone: +420 224 251 250 **E-mail:** info@spir.cz **Internet:** www.spir.cz
Bank Account: Raiffeisenbank **Acct. No.:** 375076001/5500 **Business ID:** 70108005 **Tax ID:** CZ70108005

10. **Article 9, paragraph 1 —** *Also belonging to a special category of personal data are data on convictions in criminal cases.* It is not clear why perpetrators of criminal acts should benefit from increased protection (with the exception – in some exceptionally justifiable cases – of children and juveniles). Criminal acts are acts that are harmful to society. Societal pressure arising from knowing the identity of the offender has a significant deterrent effect on continuing in criminal activity. In addition, processing data on criminal convictions may even serve as a control of the decision activities of the courts by the public and reveal judicial errors. We therefore recommend that this statement be either omitted, or that the prohibition is at least limited to only juvenile offenders.
11. **Article 9, paragraph 2, letter i)** — *allows in specific cases the processing of sensitive information (ethnic origin, health data etc.)* It would be appropriate to also add journalistic activity or freedom of expression as a reason for exception.
12. **Article 9, paragraph 3 —** *This paragraph authorizes the Commission to issue acts under its delegated powers for the purpose of further defining the conditions of when it is possible to process special categories of personal data.* We believe that such an important question should not be excluded from the competence of the European legislature and entrusted to a mere administrative body such as the Commission.
13. **Article 10 —** *provides an exception for controllers in the sense that they are not required to obtain additional information for identifying the data subject if the information they processed does not enable them to identify a natural person.* It may happen that large corporations obtain personal data for various purposes that as a whole – if they had been processed collectively and in one place – make it possible to identify an individual, but in practice such collective processing does not occur (for example a company gets information about its customer, including their e-mail address and IP address, and at the same time gets data on the number of visits from this IP address to the website, but this data is recorded separately). Article 10, however, does not make an exception for this purpose. Such a controller would then be required to aggregate all personal data in one place in order to be in compliance with the Regulation, and cannot claim the benefits given by Article 10. In practice, huge "information sets" will thus be formed, which will contain a lot of data. The possibility of misuse of such sets is paradoxically greater, since they will contain a great amount of interesting data and so be an interesting target, for example for hacker attacks.
14. **Article 13 —** *lays down the obligation to inform recipients to whom data was provided of their corrections and deletions.* Here we recommend adding among exceptions to this obligation also cases when:

    a) The changed information is made accessible in a similar manner as the original information

    b) It is evident from the nature of the matter that such special notice is not necessary. For example it cannot be required of operators of catalogs of business entities (where entrepreneur individuals are also often listed) to specifically draw attention this change in their catalog.

Registered Office: Korunní 79/1171, 13000, Prague 3, Czech Republic
Telephone: +420 224 251 250 **E-mail:** info@spir.cz **Internet:** www.spir.cz
Bank Account: Raiffeisenbank **Acct. No.:** 375076001/5500 **Business ID:** 70108005 **Tax ID:** CZ70108005

15. **Article 14 —** *This article establishes the general obligation of the controller to provide certain information to the data subject de facto automatically after its acquisition.* This obligation is too broadly worded, even despite the provisions of paragraph 5, which provides for certain exceptions from this general obligation. In particular in the case of mass services such as catalog firms the fulfillment of such obligations seems to be meaningless. It is another unnecessary burden for the data controller. We recommend deleting it.
16. **Article 14, paragraph 1 —** *Provides for the obligation to inform data subjects of the collection of personal data.* Here again an exception needs to be added for purposes of collecting data in order to exercise the right to freedom of expression.
17. **Article 14, paragraph 3 —** *sets down the obligation to provide information to data subjects about the origin of the collected personal data.* We recommended deleting it, given its possible abuse for breaking through the protection of mass media sources and given that archiving data on the origin of information is not always possible, i.e. would lead to excessive burden for controllers.
18. **Article 15 —** *requires controllers to provide information to the data subject, upon the subject's request, on data being processed about them.* This article does not include any exceptions to this obligation. Exceptions, however, should be established at least:
    a) for data that is collected for the purpose of the exercise of rights by the controller (for example for the purpose of filing a lawsuit against an entity that violates the rights of the controller, where it is not logical for such an infringer to be entitled to know everything that the controller has available concerning their illegal activity; this may the case in gathering information on cyber pirates, etc.) or
    b) for the exercise of journalistic activities.
19. **Article 17, paragraph 1, letter c)** — *This provision establishes the "right to be forgotten".* The reference in letter c) is utterly confusing, however, because the mere fact of an objection made does not determine whether the gathering of personal data is carried out *lege artis* or *contra legem.* We recommend that this provision be deleted.
20. **Article 17, paragraph 3, letter a) —** *establishes an exception to the obligation of deletion in the case that the storage of personal data is necessary for the exercise of the right to freedom of expression.* Here there should also be added the case of making information public in connection with the exercise of the right to freedom of expression (i.e. the information has already been published and will not be further published differently). It would be appropriate to also add journalistic purposes to letter c). It should also be expressly stated here that the right to deletion does not apply to cases where the deletion would disturb the informational value of a historical document. For example, a deletion of data from an electronic archive containing scans of old newspapers is technically feasible, nevertheless in practice it would mean the devaluation of the given archive and a retroactive change of the historical informational value of the given document.
21. **Article 18, paragraph 2 and 3 —** *data portability.* It can be applied, for example, to archives of e-mail correspondence or information made public on Facebook or similar social networks. The provision in its essence does not address the question of "interference" with the transmission of

Registered Office: Korunní 79/1171, 13000, Prague 3, Czech Republic
Telephone: +420 224 251 250 **E-mail:** info@spir.cz **Internet:** www.spir.cz
Bank Account: Raiffeisenbank **Acct. No.:** 375076001/5500 **Business ID:** 70108005 **Tax ID:** CZ70108005

information resulting from the nature of things, but in fact requires some business entities to implement systems stipulated by the Commission in order to make transferability possible. Given the negligible realistic impact of the Regulation upon entities established outside the Union, this will force entrepreneurs from the Union to implement these systems (i.e. make it possible for users of their services to easily cross over to the competition), while users of the services of competition outside of the Union will not have the option to cross over to services operated in the Union. As a result, the Regulation places European businesses at a serious disadvantage. Moreover, the unification of data formats will lead to significant expenditures on the part of data controllers (the necessity of changes in software systems, etc.).

22. **Article 19. Paragraph 1.** *This provision enables data subjects to raise an objection to the processing of data, unless the controller proves serious legitimate reasons for the processing.* This provision is quite unclear. To whom will the controller demonstrate serious reasons? Why should an administrator demonstrate cause, if the reason is the protection of the controller's interests against the data subject, who could in this way gain information which the controller intends to utilize (fight against computer piracy, etc.)? We recommend deleting it.
23. **Article 20, paragraph 1 —** *prohibits automated systems designed to evaluate the personal traits of a natural person or are intended for analysis or prediction of performance of work obligations.* In a similar way as provided under point 2, it should be made clear whether this prohibition applies even to cases where the only identifier of a given individual is, for example, a cookie. Furthermore, there is absolutely no reason to prohibit employers from evaluating the performance of work obligations by automated systems. The words "performance at work" should therefore by deleted. The basic problem of the provision is also the use of the term "natural person" instead of "data subject." This prohibition thus applies to any activity related to any natural person, even though this individual cannot be identified by the controller. It constitutes a fundamental restriction of existing practice on the internet, in particular in conjunction with the potential consideration of cookies as an instrument of automated data processing! Under recital 58, in addition, children are always excluded from automated data processing. The broad definition used by the Commission also covers a series of processing types that commonly take place, particularly in the internet environment, and that users do not consider harmful (common cookies, etc.). Such processing is not usually used for marketing communication, but enables users to utilize a given website more easily.
24. **Article 20, paragraph 3 —** *prohibits automated processing of special categories of data according to Article 9, without exception.* In our opinion, there is no reason for not allowing automated processing of such data if the consent of the data subjects is given. It would thus be appropriate to amend the paragraph by the addition of such a possibility.
25. **Article 22, paragraph 1**— The word "policies" used here is inappropriate.
26. **Article 23, paragraph 2 —** *Implemented mechanisms shall ensure that personal data are not normally made accessible to an indefinite number of individuals.* This requirement cannot be complied with for example in the case of internet catalogs of firms. We recommend deleting the last sentence. *Data shall be processed only to the extent absolutely necessary* – this provision does not address the question of informed consent and does not make broader processing

Registered Office: Korunní 79/1171, 13000, Prague 3, Czech Republic
Telephone: +420 224 251 250 **E-mail:** info@spir.cz **Internet:** www.spir.cz
Bank Account: Raiffeisenbank **Acct. No.:** 375076001/5500 **Business ID:** 70108005 **Tax ID:** CZ70108005

possible even with consent (see comments above under point 3.)

27. **Article 26, paragraph 2, letter b) —** *sets down the obligation, in a contract between a processor and a controller, of requiring the processor to employ only staff who have committed themselves to confidentiality or are under statutory obligation of confidentiality.* The requirement that the processor employ only staff who have committed themselves to confidentiality or who are under statutory obligation of confidentiality should be applicable only to those workers that may come in contact with personal data. We recommend modification.
28. **Article 31 —** *notification of a personal data security breach to the supervisory authority.* The obligation to notify the supervisory authority of personal data security breaches should be stipulated only for serious cases where there is a significant risk of personal data abuse. The current text of the proposal may overwhelm the supervisory authority with notices. Even in this Article 31 an exception should be provided for, similar to the exception under Article 32 paragraph 3 (but without the necessity of proving the measures taken to the supervisory authority). The notification deadline of 24 hours "if possible" (which in principle will be always) seems unreasonably stringent, in particular given the necessity of determining the extent of the security breach and verifying that a breach actually occurred. We therefore recommend deleting this deadline. In addition, it should be noted that the given notification obligation may constitute a violation of the constitutional principle "*nemo tenetur se ipsum accusare"* (no one is obliged to accuse himself.) The fact that this obligation was voluntarily complied with should therefore be at least included among mitigating circumstances in determining the amount of the sanction.
29. **Article 33 —** *data protection impact assessment.* This is in principle a duplication of Article 23. It will lead to considerable administrative burden for data controllers. We recommend deleting it.
30. **Article 35 —** *obligatory designation of a personal data protection officer for enterprises employing more than 250 persons.* A totally unnecessary institution. We recommend deleting it.
31. **Article 73, paragraph 2 and 3 —** *the right of organizations established for the purpose of protecting the rights and interests of data subjects to lodge complaints with a supervisory authority on behalf of the data subjects.* This right substantially interferes with the rights of individuals, because the given associations are authorized to lodge complaints **on behalf of the data subject,** without being obligated to seek the opinion or consent of this subject. If the given association becomes a party to the proceedings, it will also have access to personal data from the controller's file relating to the given subject without expressed consent of it by that subject. In addition, filing such a complaint may be carried out directly against the interests and will of the given data subject. Although we acknowledge the potential benefit of such organizations, their rights should be balanced and care should be taken particularly to protect the data subjects themselves.
32. **Article 78, paragraph 1 –** *Member states are authorized to lay down the rules for penalties applicable under the Regulation.* Article 79, however, contains in itself the limits for sanction amounts. We recommend that it be made clear whether Article 78 applies only to procedural rules or also to the penalty amounts.
33. **Article 78, paragraph 2 —** *determines that if the controller has established a representative, any*

Registered Office: Korunní 79/1171, 13000, Prague 3, Czech Republic
Telephone: +420 224 251 250 **E-mail:** info@spir.cz **Internet:** www.spir.cz
Bank Account: Raiffeisenbank **Acct. No.:** 375076001/5500 **Business ID:** 70108005 **Tax ID:** CZ70108005

penalties shall be applied to the representative. The purpose of this provision is not clear. If it refers to a representative in the sense of Article 25, it is appropriate to state this expressly in this provision.

34. **Article 79 —** *Sanctions and their amounts.* We consider it totally inappropriate for the structure of sanctions to be derived from turnover. Such a concept is used for example in competition law, where the impact of the unlawful conduct is actually directed at an indefinite range of consumers/customers and higher sanctions play their role, because it is not realistic for every consumer affected by the unlawful conduct to file a lawsuit and demand compensation. In the case of the Regulation, however, the impact of any misconduct is limited only to persons whose personal data it concerns, who are determinable and identifiable and who can thus claim compensation. A sanction in the amount of 2% of turnover in combination with the unclear definitions used in the Regulation, and the fact that the Regulation newly strictly regulates activities which were commonly carried by businesses for many years without in any way being called into question by the public has a discouraging character, and may lead businesses to choose a non-European jurisdiction instead, or choose not to start doing business in this segment at all.
35. **Article 79, paragraph 3 —** *the possibility of not imposing a sanction to enterprises with less than 250 employees.* While we understand the necessity of less stringent rules for small and medium companies, particularly in the Regulation, which provides a whole series of administratively demanding obligations for them, the disproportion in this provision is unacceptable. The benefit of a notice without a sanction should be granted to large enterprises as well.
36. **Article 79, paragraph 5, letter g)** *This Article makes possible the imposition of a fine of up to EUR 500,000 or 1% of global turnover to anyone who does not comply with the rules regarding freedom of expression.* This is essentially an additional sanction, complementing claims for compensation within the framework of reputation protection by persons whose rights have been interfered with by the print or electronic media. In essence, it is an instrument of follow-up censorship that can easily be exploitable. The consequences of such regulation can even be in the form of self-censorship – the media will choose rather not to write about things for which they might risk a fine. There exists a real danger of abuse of this institute by persons affected by news reporting (politicians, for example). We recommend that no sanctions be provided for in these cases, i.e. proceed according to the recommendation in point 32.
37. **Article 79, paragraph 7 —** *This article gives the Commission the right to change the fine amounts.* We believe that in such weighty matters as fine amounts should not be decided by a mere administrative body; this decision making should be entrusted to the legislature.
38. **Article 80 —** *Regulates the right of freedom of expression, while deviations are to be provided for "only" by individual member states.* This is a totally inappropriate legislative concept, whereby member states should decide on the "suspension" of the Regulation in questions regarding freedom of speech. However, these questions should be at least generally provided for by the Regulation itself, i.e. the Regulation should not apply to the exercise of freedom of expression at all.