Stowarzyszenie
Administratorów
Bezpieczeństwa
Informacji

SABI, the Association of Information Security Administrators
Al. Jana Pawła II 34 lok. 6
00-141 Warsaw
Poland
www.sabi.org.pl

Warsaw, 13 January 2010

Association of Information Security Administrators submission to Consultation on the Commission's comprehensive approach on personal data protection in the European Union

The Association of Information Security Administrators[1] is a non-governmental organization operating on the basis of the Polish Associations Incorporation Act. Its members are persons working as Information Security Administrators in organizations belonging to both the public and the private sector, as well as other persons engaged in personal data protection. The mission of the Association is to propagate knowledge on personal data protection and improve professional skills of those engaged in personal data protection. The Association has drawn up, acts in accordance with and promotes a Code of Professional Ethics of Information Security Administrators. The Association participates in the legislative process regarding national regulations on personal data protection. It cooperates with the Polish Data Protection Authority – the Inspector General for Personal Data Protection.

The Association of Information Security Administrators comprising persons engaged in the practical application of personal data protection regulations is very pleased to welcome the initiative of the European Commission to inaugurate the process aimed at increasing the effectiveness of personal data protection regulations**.** Responding to the invitation to submit contributions to the public consultation on the new legal framework regarding data protection,

[1] Pursuant to the Polish Act on the Protection of Personal Data, the term "Information Security Administrator" (Polish abbreviation for the term - ABI) is a counterpart of "Personal Data Protection Official"

the Association submits its response regarding the need to amend the Directive 95/46/EC within the scope of the personal data protection official and the Article 29 Working Party.

I. Data Protection Official

I.1 The Directive 95/46/EC needs a far-reaching reform with respect to the personal data protection official. The reform of the institution should be based on the assumption that the functioning of the official is to bring benefits to all the subjects participating in personal data protection activities:

a) to a national data protection authority, because the supervision of the compliance with the personal data protection regulations will be enhanced and partly moved from the level of the national authority to the one of the internal official;

b) to the data controller, because apart from limiting formal duties towards the national authority (as it has been up to now), he/she is subject to the changed rules of bearing responsibility for respecting data protection regulations, which may help him/her effectively adjust to the data protection obligations,

c) to the official himself/herself, for whom a better and more effective performance of duties is ensured as well as a greater stability of the function (work),

d) to the data subject who receives the assurance of a better and more effective execution of his/her rights towards the data controller.

I.2 In order to accomplish the aforementioned goals, the Directive needs to be furnished with regulations constituting an independent legal basis for the Official's activity. At the moment the Official is only mentioned in the regulations on notification (art. 18-19) and prior checking (art. 20), which is not enough from the point of view of challenges. The new regulations should ensure a consistent performance of the function of the official in all the Member States.

I.3 The essence of the proposed solution consists in the fact that what is subject to modification in the Directive are the rules of performing the personal data protection obligations within the scope of supervision exercised by the data controller (processor) and the realization of rights of the data subject. The modification consists in the official assuming some of the tasks within the scope, as referred to in points I.4-I.6.

I.4 As regards the official, the new regulations of the Directive should define:

a) his/her detailed duties which, in our opinion, should concentrate on:

- internal supervision of the observance of personal data protection regulations as well as internal organizational procedures within the scope,
- raising awareness on data protection rules of those processing personal data within an organization,
- providing assistance to the data subject in executing his/her rights towards the data controller and processor (meaning especially the technical realization of requests for information or rectification issued by the data subject)

b) rules of cooperation between the official and the national data protection authority,

c) qualification requirements to be met by the official (knowledge, experience, education)

d) specific guarantees of independent performance of the official's tasks (employment guarantee).

I.5 The national personal data protection authorities should support the Official in performing his/her duties by providing proper explanations and advice, and – at least one time for each official – training him/her in performing his/her duties. Unless it is contrary to the public interest, the national data protection authority carries out reviews of the data controller (processor) by assigning the tasks to the official. Having conducted a review, the official provides the authority with a report which contains recommendations restoring the proper legal state. The report approved by the national authority obliges the data controller to undertake proper actions. Moreover, the official is also authorised to notify the national authority of irregularities on his/her own initiative.

In the event the official acts contrary to the public interest, a national authority should have the competence to dismiss the official from his/her position.

I.6 The data subject and the official should be guaranteed the possibility to de-formalize the procedure of providing information and explanations to doubts regarding the subject's personal data processing. Compared with formal requests submitted to the data controller, such a procedure would be of preliminary nature. It would involve the participation of the official or at least necessitate his organizing the process of settling matters in his/her unit. The application of the de-formalized procedure would depend on the will of the data subject.

With relation to this, the official's personal data (name, surname, telephone number, e-mail address) should be known to the public and available on the data controller's website. What may also be given consideration is keeping a national open register of the officials.

I.7 With respect to corporations operating in different countries, it is worth considering to introduce a possibility of appointing an additional official coordinating the activities of the "national ones".

I.8 In this response we do not determine whether appointing the official should be obligatory or voluntary. We only indicate that in the event it is voluntary, the legal regulations should provide "incentives" for a data controller (processor) to appoint the official.

II. The Article 29 Working Party

The activity as well as the composition of the group should be more open to social lay participants, including organisations for data protection officials and sectors acting under codes of conduct (art. 27). In our opinion the aforementioned openness should at least consist in introducing the right of the social lay participants to:

apply to the group for adopting a stand and giving opinions during its works, which would be binding on the group (with no voting right when making decisions on the part of the lay participants).

With a copy to: Inspector General for Personal Data Protection