Warsaw, 1 February 2017

Inspector General for the Protection of Personal Data (GIODO)
Edyta Bielak-Jomaa, PhD
Stawki 2 street
00-001 Warsaw

STATEMENT
OF INTERNET INDUSTRY EMPLOYERS' ASSOCIATION INTERACTIVE ADVERTISING BUREAU POLAND (IAB POLAND) ON GUIDELINES ON THE RIGHT TO DATA PORTABILITY (IN RESPECT OF THE CONSULTATIONS PROCESS IN THE COURSE OF WORK ON THE IMPLEMENTATION OF GDPR).

Dear Madam Inspector,

in connection with the GIODO's invitation dated 20th of January 2017 issued under the consultation process in the course of work on the implementation of the General Data Protection Regulation (GDPR), hereby, I present the position of IAB Poland in this respect.

I. Preliminary remark

Article 20 of the GDPR refers to the right to data portability of data "**provided**" to the data controller by the data subject. In our opinion, "**provision**" of something requires conscious of the user activity. There is no justification for concluding that the data "provided" include any data which are generated (as it were in the background) as a result of the user's activity. The approach proposed by the Article 29 Working Party:

"The terms »provided by« includes personal data that relate to the data subject activity or result from the observation of an individual's behaviour but not subsequent analysis of that behaviour. By contrast, any personal data which have been generated by the data controller as part of the data processing, e.g. by a personalisation or recommendation process, by user categorisation or profiling are data which are derived or inferred from the personal data provided by the data subject, and are not covered by the right to data portability".

may create an interpretation issue and may cause legal uncertainty. Apparently, it is difficult to put a clear boundary between the data based on observations of user's behaviour and data deriving from the analysis of such behaviour.

II. Legal and business remarks

1. Since the data portability requires the **interoperability of the data format**, in order to avoid customer complaints as well as excessive costs for entrepreneurs, it would be advisable to agree on a standardized format/formats.

2. **It should be clear at what stage and in what form the information obligation which is recommended by the Article 29 Data Protection Working Party shall be implemented** and which concerns the provision of information on the customer's right to data portability before termination of his or her account services.

3. **Defining data generated by user's activity while using the services as data which shall be subject to transfer, has negative business implications.** For instance, in order to create a well-functioning system of recommendations, suppliers collect and analyse data concerning VOD content watched by users, the frequency of their viewing (including at what time, for how long, etc.). These data have specific commercial value to entrepreneurs such as the ability to create offers tailored to customer expectations and build customer satisfaction with the services provided to him or her. Entrepreneurs bear specific costs to collect such data, regardless of the cost of their further analysis. The question arises, whether it is at all possible to split data collected for profiling of their "assessment/analysis", as such data are often collected to provide certain services at a particular website. **Transfer of such data to another entrepreneur resulting in disclosure, in a way of know-how of the previous service provider** (which type of data it collects, by what criteria). Additionally, it implies that a new entity (provider) might no longer need to profile such user on his or her own (e.g. such provider gets a profile of user who likes watching comedies on Friday's evenings). **As a result, the transfer of such data to another entrepreneur on user's demand may be deemed to be a serious infringement of trade secrecy and fair competition.**

4. **The interpretation of the Article 29 Working Party defining data as data provided by the data subject**: data, including also meta data (so-called raw data) and all data generated by user's activity (search data, history of service, traffic data, location data) as well as data processing by data controllers, which are operating data (mostly based on system logs and statistics) – **is too broad,** and, consequently is contrary to recital 68 of the GDPR. As a result, such interpretation may cause many difficulties in application of the right to data portability on the user side (data subject).

5. Such a broad definition of "**personal data**" covering meta data, cookies etc. means that even the "technical data" are deemed to be the personal data. Consequently, telecommunications service providers and Internet service providers may face many difficulties and challenges. Apparently, it leads to copying and sharing of databases collected/created by the user. **The average consumer who requests to transfer all of his or her data is not aware of the existence of certain data in the provider's system, including the data covered by the telecommunication secrecy.** In practice, the implementation of the guidelines included in the subject document of the Article 29 Working Party implies many hazards for telecommunications secrecy. Apparently, such interpretation may be caused by misguided interpreted meaning of user's comfort in respect of data portability (e.g. on social media). It should be underlined that, as a rule, the data controller **does not process data as the data controller** (in some services only as a processor, hosting provider).

6. The examples given above include not only operating data but also statistics which **may be covered by telecommunication and trade secrecy of the data controller** (i.e. playlists which show what kind of music the user was listening to or which films were watched by him or her on VOD platform). Such a wide range of data reveals for the competitors information about provided services for the specified entity and also (because of the ease of counting singular streams according to the publicly available price-lists) it allows for accurate calculation of the income of a competitor resulting from provision of the specific service.

7. **It seems that pseudonymised data which are collected in cookies should be covered by the exemption from Article 11 paragraph 1 of the GDPR**. The purpose of processing of the data is not indicated for the identification of Internet users, but the

identification has legal basis in Article 11 paragraph 2 of the GDPR and always causes doubts about the identity of actual user of the device. Extension of the right to data portability for data included in cookies of third parties causes that it is not clear who should fulfil the obligations of a data controller. If it were service providers [whose websites and applications are used] it would rise the doubt to which other providers and what kinds of data should they provide. If the obligation should be fulfilled by third parties, it causes significant difficulties of the technical nature – according to the examples mentioned earlier – the portability of data to other entrepreneur on demand of the user could cause infringement of trade secrecy or fair competition.

8. In the opinion of IAB Poland, it should be assumed that the data processed for private purposes, should be copied and transferred **by the data subjects on their own**.

9. What might be highlighted, usually **email service providers do not usually process the data** such as contacts, address books or email correspondence, including personal data of third parties but merely hosts them for the user. What is more, these kinds of data are not generated while using the email service because of the fact that the user is preserving themselves on the devices and controller is merely hosting them in its system. All in all, the data should not be covered by the definition of personal data which are processing by controller.

10. IAB Poland would like to emphasize that even more doubts arise from example regarding payment service, purchases and other kinds of data which are connected with loyalty cards of data subjects because of the fact that **loyalty programmes with the option of online purchases are served by different types of entities and each of them usually processes the personal data in different scope** (i.e. separately the entity providing an online platform, separately shops, separately payment processor). The before mentioned subjects do not access to the statistical data of its competitors' services, in particular the payment processor does not have any grounds for sharing data from payment cards. The data about transactions may constitute in trade secrecy.

11. Furthermore, in contrary to the assumptions of GDPR, the recommendations to API for transferring and receiving data which may allow interoperability and re-use of such data, leads to the need to harmonization of tools and formats by controllers, which will **not**

always be possible due to technical barriers and significant costs of such operations. Use of the API in terms of social media or email services, according to the guidelines about portability of hosted data (not processed by the controller on the basis of contest or under the contract with the user provided to the controller) requires the necessity to adjust or amend the technology in order to enable re-use of data by data subject with the new controller.

12. In this context, there is also a doubt whether **the "generated" data would be transferred only on the explicit request of the user**? What is worthy to be noted, the data subject may not be interested in portability of the database. If the user wants to transfer his service or profile on social media to the other service provider (new controller), the user can only assume transfer of the user account which is covered by the definition in Article 20 of the GDPR i.e. data which are transferred to controller on the basis of the consent or need to fulfil the obligation arising from the contract and are processed by the controller.

13. It is not at all certain, what is the purpose of transferring of the generated and hosted data with the data provided by the data subject (the scope which results from the Article 20 and recital 68 of the GDPR), if the new controller should not process these kinds of data. In addition, we can indicate that **other numerous doubts regards the storage of data** i.e. who is liable for creating and maintaining the security zone where data should be protected before transferring to the new controller? Should the security zone be encrypted in API or in the network or on the server of the third party? What is the legal basis for these actions?

14. It should also be noted, that due to the lack of technical possibility of controlling data transferred by the API, **it is impossible to fulfil the recommendations**, that the data which are transferred before being downloaded by the new controller, should still be under the control of the data subject who file a request.

III. <u>The below presented remarks constitute other examples of issues and doubts can arise from guidelines included in the document of the Article 29 Working Party</u>

1. In case when the client files the service provider the request (or should it be a motion?) that the service provider transfers its data to the other entity (even from a different industry).
   (a) Is the service provider obliged to collect all the data which user "provided" to him or her in the broad sense in the course of the contract, i.e. personal data (e.g. name, PESEL number), data from user complaints (about illnesses, changes of address), payments (e.g. account number, credit cards). Does it include the data generated during provision of the services (e.g. billings) or its own assessments, profiling of the client for offers, evaluation of credit scores, whether to provide him or her with the information about its services (i.e. what VOD the user had bought and when), content of expressed consents, and even client responses for marketing actions, recording of all conversations with the client and just pass then to the other entity (it can be unknown service provider)?
   (b) Is the service provider obliged to verify credibility of the entity who will receive the data (if the controller is obliged to take care of the data) and shall it be entitled to refuse to transfer the data if the recipient is not credible ? Should it be entitled to reveal the telecommunication secrecy? Does the subject who received the data covered by secrecy (but not be a telecom operator, e.g. bank) is entitled to process such data only because the client requested it?
   (c) If the controller collect additional data on the basis of Article 11 paragraph 2 of the GDPR on the occasion of data processing for the purposes which do not require identification, what should be the scope of data considered as sufficient to maintain the principle of adequacy and at the same time exclude the possibility of violation of Article 20 paragraph 4 regulating prevention of adverse effect on the rights and freedoms of other people?
   (d) Should the service provider have to ask the client what kind of data he would like to transfer and indicate what kinds of data and in which form he has?
   (e) Should the client should give its consent for processing of these data by the recipient of data?
   (f) What is the purpose of transfer of the data about the client between entrepreneurs (e.g. Jan Kowalski, PESEL number)? Does the entity who received the data should verify their accuracy, completeness and the date is up to date?
   (g) Is the recipient of the data designated by the client entitled to refuse receiving of data or any part of them if the recipient knows that processing is not necessary to

fulfil the obligation arising from the contract or he knows that it does not have legal basis to process such data?

2. It should be also noted that the data portability in accordance with the interpretation of the Article 29 Working Party extended with regards to the webmail service to address books, contacts and the whole correspondence, does not only cause issues for the data controller who transfers such data (in fact that would be a copy of the data base stored for the data subject, who does not process the data), but also **triggers additional risks** including:
   (a) the new controller receiving the data should not (in accordance with the guidelines) process such data or should include it as a data collection in the service for the data subject, which means **the obligation of processing of such data collection by the new data controller**, at least for the purpose of determining, which data should not be imported to the new service. The question arises what would be the legal basis for such a processing, in particular bearing in mind the fact that the data collection includes the data of third parties who did not grant their consent nor are aware of the data transfer.
   (b) a question might arise also whether the new data controller (who downloads the data as a data collection) **is obliged to notify third parties of the processing of their data** obtained from the user? Moreover, shouldn't it be the case, that if the new controller does not process such data, the data should not be subject of the request under the right to data portability?

Sincerely Yours,

Włodzimierz Schmidt

President of the Management Board