PROTOCOL FOR ACCESS TO INFORMATION

Before applying statutes or resorting to actual legal action there are several options that enable data controllers and applicants to cooperate and facilitate unhindered access to information. Our suggestions for best practices:

1. It is very important that applicants specify the requested data as precisely as possible. This, however, is not always possible as, due to the asymmetry of information, applicants often have no knowledge of the type and number of documents prepared for a certain case. In such cases the nature and content of the requested information should be outlined in detail. It can also be useful to specify why the applicant needs the information in question, even though providing this reason is not a requirement.

2. Providing the requested cluster of data/documents/information cannot always be done within the timeframe laid out in legislation (15 days in Hungary). With adequate reason, however, the data processor can request extra time (e.g. if the amount of data to be made available is too large, especially if it is not an already prepared cluster of data but information to be collected from several sources; or if the trade secret classification should be verified). This makes it clear for the applicant that the data processor wishes to make the data available, but in order to provide accurate and quality answers (the exact and full group of data requested), it needs time. This, within certain limits, can be a compromise acceptable for both parties.

3. In the event that the applicant requests a too large amount and/or cluster of documents the data processor may offer to provide personal review and consultation, as it is possible that the applicant does not need every single piece of information (e.g. detailed technical descriptions). This can happen in cases when the request is made for all documents in connection with a certain case as opposed to concrete data. In such cases it is sufficient to make the selected materials available, saving time, money and sweat.

4. In some cases the data processor is not processing its own data but that of its client. Such occurrence is when a company submits certain data, information, documents that were classified as trade secret by the client (i.e. the company) to an authority. Based on the above described scenario, the data processing authority may decide to make the data available despite the classification because such classification by the client cannot be considered a fact. In the event that the authority does not want to take a position, it can request the opinion of an expert (e.g. a lawyer employed by the authority, an independent expert or, in some cases, the data protection commissioner).

5. The client can help the data processor to great extent by not stamping an entire cluster of documents as "trade secret" but selecting and marking in advance the specific parts classified as such, and by providing detailed reason for this classification and information on the potential negative market/economic/financial effects of making such information public. In case the client does not do so by itself, the authority can request it at the start of proceedings. This is not only advantageous for the data processor and the applicant because it facilitates data requests, but also for the clients as they can avoid their trade secrets being revealed with adequate reasoning.

6. In the event that the applicant turns to the wrong data processor with the request it is best if this is revealed as soon as possible. It is helpful if the approached data processor names the relevant authority – if they know which authority it is. If the data processor denies the request with reference to trade secret and later tells the applicant in court that it is not the relevant data processor, it is a sign of lack of good faith and will to cooperate.

7. Dialogue, consultation between the data processor and the applicant can be useful in a lot of cases. This method can be more effective than automatic refusal for straightening out misunderstandings or questionable cases, but also for sharing information that may not exist in writing. The applicant should also consider – especially when requesting a large quantity of information or information of the more sensitive kind – initiating consultation for the success of the data request. The applicant can, in the course of the consultation process, inform the data processor what is needed and why. Thus the data processor will not only see a formal request but can become familiar with the intent of the applicant. The data processor can take position based on this intent and can decide on the quantity of information to make available, and can initiate further dialogue. This can prevent a lengthy court procedure that is not in the interest of either party but is possibly more adverse for the applicant due to the time loss that can amount to years. As the court may order the data processor to make available the data that could have been obtained by the applicant through dialogue, consultation has great potential to facilitate a win-win situation. If communication between the two parties is difficult or unfruitful the involvement of an independent middle-man, a so-called mediator can provide a solution in facilitating the successful data request.

8. The above points show that a positive approach on both the data processor's and the applicant's part is one of the most essential elements of a successful data request. Good intention and understanding is necessary on both sides: the applicant's aim is not to hassle the data processor or to go to court, but to get to know information – but in order to do that the applicant should also make compromises sometimes (e.g. about deadlines) and actively cooperate with the data processor.

9. Resorting to legal action should be the last step. The Energiaklub's data requesting philosophy shows that our requests for data are not l'art pour l'art, that is, our goal is not to bring the issues to court. It is also important that in sensitive, ambiguous legal situations the applicant has the opportunity to turn to the data protection commissioner. It should be mentioned, however, that In Hungary, according to section 1 of paragraph 27 of the act on data protection, "*Anybody may turn to the commissioner for data protection if in his or her opinion he or she suffered infringement of the law in relation to exercising his or her rights relating to the management of his or her personal data or his or her access to data of public interest, or if he or she considers that there is an imminent danger of such infringement, except where a court procedure is underway with respect to the case concerned.*". It is at the discretion of the applicant to decide whether to choose legal proceedings first and then turn to the commissioner, or the other way around, or only use one of the methods.