Spolek pro ochranu osobních údajů

Spolok pre ochranu osobných údajov

General comments

The Czech and Slovak Data Protection Associations are the largest and oldest associations dealing with the processing of personal and other data in the Czech Republic and Slovakia. Its members include both Data Protection Officers and other data processing professionals from both the private and public sector.

We welcome the opportunity to jointly present our comments to the recently published EDPB draft of Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR.

We would like to point out that these guidelines are crucial for the success of Europe's digital economy. This is even more important given the current inability to really boost Europe's data-driven economy and the increasing reliance on foreign (non-European) data services we see in practice. In light of the legislative "storm" in recent years (DSA, DA, DMA, AI Act, DGA etc.), it is very important to set up a data processing regime, and in particular a personal data processing regime, which will convince data controllers and processors that the European Union offers a balanced, stable, predictable and development-friendly environment for the data economy. Therefore, in particular the level of administrative requirements that may unduly burden data controllers should be carefully considered.

Furthermore, from the perspective of the interpretation of the processing of personal data on the basis of legitimate interest, we consider the interpretation of two aspects - the principle of necessity and data minimisation - to be very important. Unfortunately, in our view, the proposed guidelines do not adequately address neither of them. **Within the interpretation of the necessity element, we consider essential to highlight the cost aspect.** The cost of less invasive measures (compared to personal data processing) should in some cases be one of the important considerations that controllers should be entitled to take into account when carrying out the balancing test.

We would like to point out, that the guidelines do not address one of the most frequented areas of bulk processing of personal data under 6(1)(f) GDPR, namely the processing of personal data resulting from EU Directive 2019/1024, on open data and the re-use of public sector information. The repeated processing of public sector information, and especially the processing of the so-called Open data is one of the priorities of the EU, as evidenced, for example, by the newly created concept of high-value datasets. Given that the value of the European public sector data processing (PSI) market is in the hundreds of billions of euros per year and is constantly growing, and this area of processing is based almost exclusively on legitimate interest, it is surprising that this topic has been omitted.

Detailed comments

Point 9 - restrictive interpretation of the legal basis for processing. We cannot agree with the view expressed by the EDPB that "*Rather, it should be recalled that Article 6(1)(f), like each of the legal bases set out in Article 6(1) GDPR, must be interpreted restrictively*" because this conclusion has no legal grounds in the GDPR on in the EU law in general. The primary corrective for the appropriate use of this legal basis is the „necessity“ aspect, as expressed in the individual points of Article 6(1). However, the GDPR in no way implies that the legal bases for processing should themselves be interpreted restrictively. On the contrary, such an unreasonably extensive interpretation contradicts both the quoting provision in rec. 4 and the needs of the digital economy. In other words, the aim of GDPR is

not to prohibit or prevent the processing of personal data (it is not a regulation **against** processing), but rather a regulation which protect the rights and interests of data subjects **within** such processing.

Point 12 - requirement for careful assessment. In practice, controllers carry out an assessment of the fulfilment of all 3 aspects listed in point 6 where large-scale processing which should last a long term is involved. Therefore, it is appropriate to insist that the controller's decision is "*documented by the controller in line with the accountability principle set out in Article 5(2) GDPR*". However, we must point out that in common practice a number of particular balancing tests are carried out which are not realistic to be documented in writing (see for example the example given in the comment on point 71). This may be a normal one-time processing (sometimes related to the compatibility of purposes assessment under Article 6(4) of GDPR), such as in the case of transmission of data to public authorities in the event of suspected law infringements. In such cases, it is neither common nor appropriate to fully document the controller's decision in writing, as this would impose a significant burden on the controller. Suitable internal processes, such as a workflow in which the business owner, lawyer or DPO approves the processing, should also be considered sufficient documentation of the balancing test in these cases when properly set-up and documented. A number of similar cases arise in practice. The issue of documenting the balancing test should therefore be approached in a sensible manner and only required where it makes sense and does not unduly burden the controller.

Point 13 - Necessity requirement. Here we would like to highlight that the GDPR links legitimate interest to the processing being "necessary", not "strictly necessary" to fulfil it. If the EDPB extends the necessity requirement to one of "strict necessity", it does so entirely outside the scope of the statutory text, EDPB tries to establish new obligations with no basis in the GDPR and this approach and interpretation may undermine the development of Europe's digital economy. The strict necessity requirement is only mentioned in the GDPR in some recitals with respect to specific situations. In the statutory text, it is rather linked to the requirements of Directive (EU) 2002/58, but not to the GDPR.

Point 17 - requirement to declare legitimate interest. In our view, it is not possible to link the existence of a formal declaration of legitimate interest in a document with the material requirement of fulfilling Article 6 of the GDPR (i.e. the existence of legitimacy of legitimate interest). A lack of declaration of a legitimate interest may affect, for example, the fulfilment of the transparency requirement, but not the existence of a legitimate interest as such.

Point 18, example 2. Here, unfortunately, it is not clear whether the EDPB considers the phrase "for the greater good of society" or the phrase "to monitor possible criminal activities in the area" to be an expression of legitimate interest. While the first sentence does not fulfil the requirement of specificity, the second sentence is clear as to the purpose of the processing and therefore seems to us to be sufficient in terms of the requirement of specificity (which does not necessarily mean that it will always be legitimate).

Point 18, example 3. We consider this example to be not fully clear formulated. It omits other aspects, such as whether the database of former subscribers is not also stored for the purpose of records of contracts or bookkeeping, how specific the intention to publish a new magazine in the future must be, etc.

Article 19. We recommend adding that *'the interest pursued by the controller should be related to the actual or **specifically planned** activities of the controller'*. See also the previous point.

Point 46. Here we are not clear on the meaning of the part of the sentence "*or realizing that it has been misused or compromised.*" How should the controller take into account these facts (we understand that the likelihood of some potential personal data breach and misuse is meant here)? To what extent should the controller assume that they will or can occur (the risk of misuse always exists and is inherent in principle in any processing of personal data)?

Point 53. We consider the conclusions set out here to be somewhat simplistic. Proper compliance with the information obligation will always lead to the data subject being aware that his or her data will be processed. In particular, the level of such information can then certainly contribute to the fulfilment of the „reasonable expectation condition".

For the sake of completeness, we add that EDPB refers here to Guidelines 8/2020 on targeting social media users, version 1.0, which is outdated and replaced by version 2.0.

Paragraph 54, Example 5. With reference to the CJEU judgment in the case C-252/21, we recommend mentioning also the text of paragraph 122 of that judgment, which in our view clarifies the matter further.

Paragraph 54, Example 6. We do not think that this example is entirely appropriate, since in this case it is also (and, from a certain point of view, primarily) an interference with a personality right under civil law.

Paragraph 57. Although we generally agree with the EDPB's view in that point, we believe that the very fact that the GDPR imposes a high standard of data protection can be taken into account (in favour of processing, e.g. in the area of data security) when performing the balancing test.

Paragraph 68. We would like to point out that no provision of the GDPR (nor Article 5(2) GDPR) implies an obligation to provide a balancing test to data subjects, even upon their request under Article 15. Furthermore, the balancing test can include internal and/or sensitive information, for example about technical and organizational measures implemented to fulfill the data integrity principle. Making these information public may lower the level of data protection and efficiency of the security measures.

Point 71. Here, the EDPB appears to misinterpret the legal construction of the objection. Leaving aside the objection to processing for direct marketing purposes, the objection is intended to serve the purpose of having the controller take into account the specific situation of particular data subject. An objection that does not contain a description of the specific situation is not an objection within the meaning of Article 21 (because it does not meet the content requirements of an objection) and certainly does not trigger any obligation on the controller to reexamine or re-perform the balancing test.[1] The controller is also not obliged to ask the data subject whether there happens to be a specific situation that he or she could have invoked - it is the data subject's responsibility to properly

[1] Only an objection which contains a description of such a specific situation will trigger the obligation to re-perform the balancing test, but only in relation to the data subject who raised the objection, taking into account the facts objected to by him. An example could be the processing of employee photographs on ID cards. The controller has carried out a balancing test and the result has allowed the processing. However, a particular data subject objected that his photo shows his face affected by a skin disease and it is not reasonable to process this photo (for these purposes, we leave aside the assessment in the light of Article 9 GDPR). The controller is therefore obliged to take this into account and to perform a new balancing test only in relation to this data subject and his/her objection and specific situation.

substantiate his or her objection. Therefore, an objection that does not contain any indication of a specific situation of the data subject may be rejected by the controller without further consideration. Only if it is obvious for the controller that the data subject wished to invoke his or her particular situation, but that this is not properly described in the objection, could the controller be obliged to ask for a further information. This misinterpretation is partly reflected in paragraph 78, where it should be noted that the legislator merely used a reference to the terms of Article 21 in Article 17(1)(c) GDPR.

Point 85. Although we generally agree with the EDPB's view in that point, it should be added that the assessment of accuracy and completeness should also be carried out also with regard to the source from which the personal data were obtained (taking into account, of course, the purpose of the processing). For example when personal data from public registers are processed for purposes which involve further disclosure of such data, the rectification of the data cannot be carried out in the context of this derived processing because its purpose requires the processing of data which are accurate in relation to the source register (even if inaccurate data are processed therein).

With regard to **point 93**, we would appreciate more insight from the EDPB on how to take into account in the balancing test, for example, the fact that some of the data subjects whose data will be processed may potentially be children, but the majority of the data subjects will clearly be adults.

Point 95. Regarding the reference to the DSA, we only note that it is a sector specific regulation, so drawing conclusions from the lex specialis on entire European law may not be the most appropriate approach.

Point 105. While we agree in principle that controllers should be transparent about the types of fraud (fraud threats) they wish to prevent as specific as possible, we note that in practice it will not always be possible to specify these in more detail or to indicate which specific data will be taken into account in this way. In our practical experience, the types of fraud can be very diverse, they change very quickly over time and de facto all processed data can be used to detect them, particularly in the area of cybercrime, vishing, phishing etc.

Paragraph 129: We understand the EDPB's statement that controllers should not process data for the sole purpose of systematically detecting crime. However, if such processing is combined with other 'core' processing as an ancillary activity, like client's identification, service providing etc., then in our view there is nothing to prevent controllers from reporting any breaches detected.

We are grateful for the opportunity to provide our comments on the draft Guidelines.

JUDr. Vladan Rámiš, Ph.D.
Mgr. František Nonnemann
Ing. Václav Mach
Members of the Committee
Spolek pro ochranu osobních údajů

JUDr. Lucia Semančínová
JUDr. Pavol Szabo
Members of the Committee
Spolok pro ochranu osobných údajov