Spolek pro ochranu osobních údajů

Comments on the EDPB's proposal of "Guidelines 07/2020 on the concepts of controller and processor in the GDPR" Version 1.0

We welcome the opportunity to present our comments to the recently published EDPB draft Guidance on Controller and Processor. In general, we are pleased to note that despite the fact that all the attention is mainly focused on the fight against the global pandemic situation, the EDPB still follows its tasks in the field of the consistent application of the GDPR and issues these long awaited guidelines in this direction. Even though the concept of the controller and processor has not changed in substance since the Directive 95/46/EC and since the WP 29 guidance in opinion 1/2010 (WP169), we all feel the need to address this issue reflecting the latest trends.

As a general comment we believe that the draft guidance accurately reflects the existing situation with regards to the position of the data controller and processor. It usefully clarifies the main principles of the approach to be taken into consideration whilst performing an assessment of the position of the parties involved in the personal data processing activity.

In detail we hope that the following **specific comments** are helpful to further improve this important guidance:

FUNCTIONAL CONCEPT

We endorse the functional (instead of formal) approach taken by the Guidance as it gives more room for an assessment of each specific situation the controller/processor might be in and subsequent rights and obligations deriving from it. It seems especially consistent with recent CJEU decisions on joint controllership. On the other hand, it places a burden on the party involved in data processing in the way that might in practice lead to a situation where the regulatory authority might assess the situation differently and reach different conclusions from the party. We believe the principle of accountability will play a significant role here and the decision of the party involved in personal data processing should be based on an expert assessment where the factual situation will be the driver of the final decision on the party position. The context of data processing, as mentioned in the GDPR, plays an important role in deciding on procedural activities and should not be underestimated by either party involved in the data processing activity.

Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat at the address Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: 296210562

IMBALANCE OF POWER

We can only agree with the fact that the imbalance of power between processor and controller does not discharge the controller from its obligations under GDPR, on the other hand we would like to recall the fact that in practical life and contract negotiations the controller might face challenges in this direction whilst negotiating with a big global player. Reflecting this situation GDPR placed several obligations to both controllers and processors. To be fair, the responsibility for these obligations should be attributed to the party being in a more powerful position.

CONTROLLER

We fully support the concept of the essential and non-essential means decision being left to the processor whilst still remaining in the position of a controller. We believe it accurately reflects the existing practice.

PROCESSOR

- In section 81 you provide a good example of supplier which, whilst delivering external IT support (with fixing the bugs), still does not hold the position of a processor because his task is not processing personal data, and access to personal data within the engagement might be purely incidental. Should not a similar approach be applied towards the suppliers of external IT services consisting in e.g. vulnerability or penetration testing? This leads to the suggestion of listing typical examples of the mentioned cases.

- The EDPB recommends the parties to negotiate and agree in the contract the consequences of the notification of an infringing instruction sent by the processor, and in case of inaction from the controller in this context. One example would be to insert a clause on the termination of the contract if the controller persists with an unlawful instruction (Section 149). The right of the processor to terminate the contract based just simply on the "declared unlawfulness" of the controllers' instruction might easily be misused and in general may undermine the role of the data processing agreement. The recommendation and its practical implications should be considered in more detail.

- Section 107 provides that *„...The controller must evaluate the terms and in so far as it freely accepts them and makes use of the service, it has also accepted full responsibility for compliance with the GDPR. Any proposed modification, by a processor, of data processing agreements included in standard terms and conditions should be directly notified to and approved by the controller. The mere publication of these modifications on the processor's website is not compliant with Article 28."* The aforementioned provision is contradictory to some jurisdictions e.g. the Czech Civil Code[1] which allows to change contractual conditions by publishing the changes on the web (with a given term for the contract withdrawal by the other contractual party who does not accept the proposed change). We believe the situation might be similar in other EU jurisdictions. In this context we would like to suggest adding examples from different member states for comparison.

- In the example in Section 42, we consider that the nature of the relationship between the two companies will depend primarily on the circumstances of the processing (functional approach). E.g. it might also be argued that, market research agencies that

[1] Section 1752 of the Civil Code

have their own network of respondents to whom they ask questions that are of interest to the clients of these agencies which will usually be separate controllers of personal data.

- In the example given in Section 59, we would appreciate it if the EDPB could express its opinion on the position of “ordinary users” of social networks, e.g. natural persons who set up their own private site on such a network. At the same time, it would be appropriate to address the issue of joint controllership of the social network operator and the relevant founder of the account on this social network, if this founder is a public body, incl. EU institutions. Joint responsibility in these cases may raise a large number of legal issues.

- With regard to the example concerning 'Headhunters' in Section 66, we would like to point out that this case could also be considered a combined relationship in which Company X would be partially a separate controller and partially a processor for Company Y. Without further explanation of the sentence: “Even though they have not formally taken a decision together, Companies X and Y jointly participate to the processing with the purpose of finding suitable candidates based on converging decisions: the decision to create and manage the service “global match” for Company X and the decision of Company Y to enrich the database with the CVs it directly receives”. We believe in this case it would be difficult to infer joint controllership.

- In connection with Section 76, we would appreciate EDPB to express its opinion on the extent to which Article 29 also affects external workers (other than employee or interim staff provided via a temporary employment agency) cooperating with the controller on the basis of a commercial contract where the position of such worker is close to that of employees. E.g. whether such external workers will always be considered processors or may hold a position similar to employees (and then be covered rather by Article 29 than by Article 28). See also section 86.

- We believe that the requirement for the controller to be entitled to request changes to the service provided raised in paragraph 82 should apply in all cases to the scope of the data being processed (incl. the time of their storage), not to all aspects of processing. In practice, for example, for services that consist in providing a pre-programmed IT system, it cannot be considered realistic that each customer (controller) could request programming of changes in the system without the approval of the supplier (processor). Such a requirement (resulting per se only from the existence of a data processing agreement between the parties) is in practice unrealistic (especially in cases of a black-boxed solution with minimal interaction within the controller´s IT system).

- With regard to the second bullet point of Section 111 we believe that there is nothing to prevent processing (and processing contracts) from being concluded for an indefinite period.

- Section 122 et seq. - we do not believe that Article 28 of the GDPR should be interpreted in the way that the processor is in any case obliged to ask the controller for consent to change the level of security measures during the time of processing according to a previously concluded contract with the controller. The fact that GDPR in Article 28 (3) (a) provides that the controller is entitled to give processing instructions to the processor, whereas in point (c) there is envisaged (only) a general obligation for the processor to take all measures required under Article 32, shows that GDPR does not require the controller being entitled to directly instruct the processor on specific security measures (this, of course, does not exclude that such an obligation could be

contractually agreed). This is mirrored in Art 32, where the decision on appropriate measures is attributed also to processors. In practice, the need to follow all the instructions of the controller regarding security measures could in some cases cause unsolvable dilemmas for the processor. First of all, this may affect the processors who offer their own prepared IT system, where it is not possible to determine security measures for each controller separately. In addition, should the controller be (directly from a data processing agreement and GDPR) entitled to require such measures without any limitation even after concluding of DPA, it could result in a risk of a disproportionately high investment on the side of processor without the possibility to influence the number of this steps or related cost. Nor it can be overlooked that Article 32 lays down the corresponding obligations not only to the controller but also directly to the processor, so there is no need to instruct the processor to take specific steps, because the processor has a direct binding legal obligation to do so.
We therefore consider that in order to fulfil the obligation under Article 28 (3) (c) GDPR it is indeed sufficient for the processor to undertake (generally) to take the measures provided for in Article 32.

Of course, in a number of cases (especially in the case of high-risk processing), it is appropriate from the controller's point of view to insist to be authorised to impose further specific instructions on security measures to the processor. Such an arrangement would then be part of the contract and would be rather a contractual obligation on the part of the processor, than an obligation arising directly from the GDPR.

However, we agree that the explicit written overview of such measures when concluding the DPA could in some cases be an appropriate step. This mainly would necessitate documenting the decision under Art 28 (1), regarding Art 5 (2). From a practical point of view, however, we cannot recommend that an overview of these measures should be part of the data processing agreement or its annex, as any change to these security measures would require a change to the contract, which is very impractical and in many cases unrealistic (critical state IT systems).

- Section 141 – due to regular discussions and questions we had during the last years, we would recommend explicitly stating that the controller and the processor may agree that the controller could be obliged to pay a reasonable fee for the processor´s assistance in audits, unless the amount of the fee is obviously designed in the way that could discourage the controller from carrying out such audits. Pricing is beyond the scope of the GDPR. We on the other hand definitely see cases where pricing and costs are used as forces to avoid any personal inspection and undermine the right of controllers, and clearly see this as unlawful practice.

- The right to inspect sub-processors (section 141) may also lead to an obligation to inspect the subprocessors. It might be possible to rely on inspections of the processor. A more decisive position to this question may also be helpful in practice.

JOINT CONTROLLERS

Usefully a lot of room is provided to the guidance on joint controllership. The concept was newly introduced by the GDPR (Art.26), however no detailed guidance was provided. Sections of the guidance might already be read as hints on sections of an arrangement. Given the historical development of processor contracts, we will soon reach a level of clear guidance of required topics in the arrangement (similar to Art 28 (3)). We already see JC-Contracts with very little detail. Some of them in reaction of the CJEU decisions. These are bound to the

requirement of "laying out in transparent manner", which in our opinion leads to a certain amount of explicitness. Clearly stating that the list of subsections of this chapter of the guidance should be read as topics needed to be agreed in contract would help to improve many contracts in practice.

We very much appreciate the explanation and the many good examples given in these Guidelines as joint controllership as a new concept is rarely reflected in the contracts and it may simplify things. In particular, the area of clinical research has been waiting very patiently for your Guidelines. Under points 3.2.2.1 [Jointly determined purpose(s)] there are important examples described such as general *Research project by institutes* (Section 66, page 21), which is quite clear. On the other hand *Clinical Trials* example seems not to be fully thought through, because in reality it is one of the most complicated and sophisticated relationships involving the rules of the *Sponsor*, plus the *CRO* (*Contract Research Organisation*), *Study Site* (*Hospital and its patients*), *Principal Investigator (PI)* and his Study team. Clinical trials may truly affect the whole world (it means that Sponsor could be an Indian Company responsible for processing health data of an EU patient, and the CRO could be a US partner of the Sponsor at the same time (real case)). The example in the Guidelines puts great emphasis on drafting the Protocol and omits the key role of *Principal Investigator (PI), and medical doctor.* In academic studies the authorship of the Protocol, with all its related responsibilities, is the *PI´s*. In these cases, in our opinion, it is difficult to think of a *Study Site* as a processor.

In commercial studies it is highly recommended to consult the Protocol with *PI* as well.[2] *PI* is the person which includes the patients into Study, he is who informs them about their rights and gives them the *Informed Consent* form to sign, he is who submits the study documentation to *Ethical Committee*, while the Sponsor submits the study documentation to the regulatory authority (*State institute for Drug Control in the Czech Republic*). *PI* is the person who in case of any serious adverse event or serious adverse reaction could indicate the change of Protocol. In most cases *PI* is the *Study Site (Hospital)* employee. It leads us to believe that Sponsor and Study Site (disposing by PI) will be usually joint controllers.[3] According to our information, the Dutch Data Protection Authority issued an opinion on this issue in the same sense. This concept facilitates, inter alia, the communication between contracting parties of specific clinical trial (Sponsor, representative of the Sponsor in the EU, CRO, and Study Site/PI) with the data protection supervisory authority of the concerned EU member state where the data subjects are located, because Study Site is usually located where the patients are while Sponsor could be seated overseas.

[2] See the detailed segregation of duties between Investigator and Sponsor in Guideline for good clinical practice E6(R2) issued by European Medicines Agency

[3] See also Datenschutzkonferenz,"Kurzpapier Nr. 16 Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DSGVO. Available at https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_16.pdf

RECIPIENTS

Recipient is defined as “anyone who receives personal data”, possibly a controller, processor or a third party. The example provided in Section 90 is a case of data sharing between two independent controllers. We would find it useful to provide more examples of the “third party” recipient of data, both in the public and the private sector.

We are grateful for the opportunity to provide the above-mentioned comments on the Guidelines.

Spolek pro ochranu osobních údajů