New controller-processor guidelines: beware of impact on data processing agreements

Mr. Vincent Wellens
Partner
Vincent.Wellens@nautadutilh.com

Armed with useful flowcharts to help organisations determine their role, the European Data Protection Board (EDPB) has published new guidelines on the concepts of "controller", "processor" and "joint controller". Just over a month ago, the Litigation Chamber of the Belgian Data Protection Authority had published a decision in which it appeared to adopt an extensive interpretation of the concept of "controller"; now, thanks to extensive developments by the EDPB, that interpretation no longer seems to be relevant.

In this newsletter, however, we wish to focus on other aspects of the EDPB's controller-processor guidelines, namely its considerations regarding contractual arrangements between controllers and processors and their compliance with the General Data Protection Regulation (GDPR).

Controller-processor agreements: what do we see today?

In 2018, many organisations throughout the European Union and beyond were led to negotiate on data processing issues for the very first time. Evolving best practices and creative clauses have since led some to review their controller-processor agreements (typically called data processing agreements); now, the new EDPB guidelines may prompt many more organisations to adapt their agreements.

Today, data processing agreements take many forms, from a simple rehashing of the key requirements of Article 28 of the GDPR to detailed contractual provisions. Some have detailed security requirements included, while others merely repeat the general requirements of Article 32 of the GDPR; some refer to a service agreement to describe the key characteristics of the processing (subject-matter, duration, nature, purpose, etc.), while others contain a dedicated annex describing these items. We have seen organisations use short data processing agreements, with very little detail, for (in their view) low-risk processing activities entrusted to processors, and highly detailed data processing agreements for data-intensive or higher-risk

activities. And not all of these agreements are deemed worthy by the EDPB.

"Strict minimum": insufficient according to EDPB

In its controller-processor guidelines, the EDPB states the following in relation to the content of data processing agreements:

"[t]he processing agreement should not […] merely restate the provisions of the GDPR; rather, it should include more specific, concrete information as to how the requirements will be met and which level of security is required for the personal data processing that is the object of the processing agreement".

This suggests that strict minimum clauses are insufficient in the eyes of the EDPB. To a certain extent, this is not unexpected – certain local authorities had already suggested that this might come. However, it does raise the question of how much detail will be considered sufficient to be "more specific, concrete information as to how the requirements will be met" – and whether this will in practice make life more difficult for organisations that do not yet have a clear negotiating strategy regarding data processing issues.

General considerations on the contractual negotiation and lifecycle

The controller-processor guidelines contain various general considerations regarding the negotiation and further changes to data processing agreements:

- **Signatures**: In its guidelines, the EDPB states that "[t]o avoid any difficulties in demonstrating that the contract or other legal act is actually in force, the EDPB recommends ensuring that the necessary signatures are included in the legal act". Signing remains important for enforceability and evidence reasons, but it is unclear what led the EDPB to raise this issue. Where the data processing agreement forms an annex to the (signed) service agreement, for instance, there is no reason under most laws (in particular Civil Law systems such as Belgium, Luxembourg and the Netherlands) to require this provided that the parties can demonstrate the contents of the data processing agreement at the time of signature – in particular if the service agreement itself provides that the annexes form an integral part of the agreement or otherwise foresees that signing the service agreement is deemed to be a signature of the agreement as a whole.

- **Changes to processors' standard terms**: While an imbalance of contractual power might permit certain processors to impose their terms for data processing agreements, without this changing their role as processor, the EDPB wishes to ensure that this imbalance of contractual power does not lead to unilateral changes without approval. According to the EDPB, "[a]ny 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".

Key EDPB requirements in terms of content

According to Article 28 of the GDPR, data processing agreements must include a description of the processing activities (subject-matter, duration, nature, etc.) as well as a range of specific obligations for processors. The EDPB discusses each of these requirements in turn in its guidelines:

- **Description of the processing activities**: The EDPB states that the description of the processing activities must "be formulated with enough specifications". For instance, on the types of personal data processed, the EDPB states that they should be specified "in the most detailed manner as possible", not limited to e.g. "personal data pursuant to Article 4(1) GDPR". In relation to special categories of data, the EDPB states that the contract "should at least specify which types of data are concerned, for example, 'information regarding health records', or 'information as to whether the data subject is a member of a trade union'". In practice, it may not always be possible to anticipate all categories of personal data and of data subjects perfectly, in particular in cases where a data subject might – on his or her own initiative – provide personal data belonging to categories not previously anticipated. However, the EDPB clearly expects organisations to consider these aspects carefully.

- **"Instructions"**: While processors can offer a standardised service, they must also take into account any "specific instructions on storage periods, deletion of data etc." issued by the controller. Such instructions "can include permissible and unacceptable handling of personal data, more detailed procedures, ways of securing data, etc." and a mechanism should be foreseen "for giving further instructions" (which could e.g. be by e-mail, "as long as it is possible to keep records of such instructions"). The issue of "instructions" often gives rise to difficulties for controllers: does acceptance of an offer by a processor and the transmission of personal data with the request to perform the service constitute a sufficient "instruction"? The EDPB does not respond to this question directly, but its examples suggest this approach is indeed correct. In this context, we recommend being as detailed as possible, whether you are a controller (in the request for proposal or order sent to the processor) or processor (in the offer submitted to the controller).

- **Confidentiality**: According to the GDPR, the processor must ensure that the persons authorised to process the personal data have committed themselves to confidentiality or are

under an appropriate statutory obligation of confidentiality. The EDPB states that "the processor should make the personal data available only to the [employees, temporary workers, etc.] who actually need them to perform tasks for which processor was hired by the controller". Surprisingly, the EDPB adds that the confidentiality obligation "must be sufficiently broad so as to encompass […] the details concerning the relationship", which if interpreted broadly could imply a prohibition for the processor's employees etc. to mention to anyone that they are processing personal data on behalf of the controller. From a security perspective, it is clear that talkative employees are an attack vector; we do not believe, however, that the EDPB meant to prevent (company) name-dropping for business development purposes.

- **Security**: Processors, just as controllers, are required to take "appropriate technical and organisational measures to ensure a level of security appropriate to the risk" in accordance with Article 32(1) GDPR, an obligation that covers both cybersecurity and physical security. The EDPB states in this respect that "[i]n order for the controller to be able to demonstrate the lawfulness of the processing, it is advisable to document at the minimum necessary technical and organisational measures in the contract". Later, the EDPB states that "[t]he contract needs to include or reference information as to the security measures to be adopted" – which the EDPB describes further as being either the "minimum security objectives" or detailed "security measures" depending on the specific circumstances. In any event, this information "must be such as to enable the controller to assess the appropriateness of the measures pursuant to Article 32(1) GDPR". In practice, it has become over the past two years easier for controllers to require from processors a description of the security measures they apply in any case, but controllers must bear in mind that any additional or controller-specific requirements often lead to negotiations.

  The EDPB includes in its guidelines various additional considerations on security, some of which may not even feature today in certain detailed data processing agreements. For instance, the contract should include "an obligation on the processor to obtain the controller’s approval before making changes, and a regular review of the security measures so as to ensure their appropriateness with regard to risks, which may evolve over time".

- **Appointing of sub-processors**: Under the GDPR, controllers can permit processors to appoint sub-processors in two ways: either a specific authorisation to work with a given sub-processor, or a general authorisation to appoint sub-processors in general. In the latter case, the processor must first inform the controller of any change of sub-processors (according to the EDPB, this is an obligation to "actively [indicate] or [flag] such changes toward the controller") and give the controller the opportunity to object. The EDPB states that the data processing agreement should set out the process for dealing with this (in particular "details as to the timeframe for the controller’s approval or objection and as to how the parties intend to communicate regarding this topic"). In practice, clauses regarding

the conditions for objections have become commonplace (so that objections made without justification are disregarded), so the EDPB's recommendations here are unlikely to affect contracts that are already detailed in this regard.

The EDPB states further that "[i]n order to make the assessment and the decision whether to authorise subcontracting, a list of intended sub- processors (including per each: their locations, what they will be doing and proof of what safeguards have been implemented) will have to be provided to the data controller by the processor". In other words, there is no difference between a specific authorisation and a general authorisation at the start of the contract in the eyes of the EDPB. Instead, the main difference is that during performance of the agreement, the processor with a general authorisation to appoint sub-processors can rely on silence to go ahead with its sub-processing plans (while a processor relying on a specific authorisation would need to have specific and written confirmation from the controller to go ahead). In any event, a list of approved sub-processors should "be kept up to date", states the EDPB.

- **Assistance with data subject requests**: The EDPB does not wish contracts to merely indicate that the processor has to provide assistance "by appropriate technical and organisational measures, insofar as this is possible" (as per Art. 28(3) GDPR). Instead, the EDPB states that "[t]he details concerning the assistance to be provided by the processor should be included in the contract". In some cases, this might be limited to "promptly forwarding any request received", but it might also lead to more technical duties (e.g. extracting data to assist in responding to a data subject access request). This means that when drafting a data processing agreement, the controller must anticipate the precise level of assistance – knowing that the processor will likely require compensation for such assistance if it is given a detailed description thereof.

- **Assistance with security requirements, data breaches and DPIAs**: According to Art. 28(3) GDPR, a data processing agreement must stipulate that the processor "assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor". These articles cover security requirements (Art. 32 GDPR), the response to data breaches (Art. 33 & 34 GDPR), data protection impact assessments ("DPIAs", Art. 35 GDPR) and prior consultation of the supervisory authority in the event where a DPIA concludes that there is a high risk (Art. 36 GDPR). According to the EDPB, "the agreement should contain details as to how the processor is asked to help the controller meet the listed obligations". In particular, on data breaches, "[t]he EDPB recommends that there is a specific time frame of notification (e.g. number of hours) and the point of contact for such notifications be provided in the contract. The contract should finally specify how the processor shall notify the controller in case of a breach". In practice, data breach clauses with a specific timeframe (e.g. 48 or 72 hours as from the determination that a data breach relates to the personal data processed on behalf of a given controller) are commonplace today, but it

remains important to ensure the rules are workable for both controller and processor.

- **Return or deletion of data upon termination**: A data processing agreement must state, according to Art. 28(3) GDPR, that "at the choice of the controller, [the processor] deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies". In practice, the provision of an up-to-date copy of all personal data (followed by secure destruction of the data by the processor) is the preferred avenue for most controllers at the end of a long relationship with their processor, but deletion without return of data is a simple solution for some cases (e.g. where a processor receives address lists to dispatch mailings, then deletes the address lists upon completion of the assignment). The EDPB states that the choice can be made at the beginning (in the contract), provided the controller retains the possibility "to change the choice made before the end of the provision of services related to the processing" – and that this is specified in the contract.

- **Evidence of compliance and audit possibilities**: Based on the general obligation of assistance in relation to compliance, the processor must "[make] available to the controller all information necessary to demonstrate compliance with the obligations laid down in [Art. 28 GDPR] and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller". A key practical issue that arose for processors related to their record/register of data processing activities (Art. 30 GDPR), as controllers started to demand a copy thereof. Processors do have other ways of showing compliance, though, and the EDPB suggests as much, stating that "the relevant portions of the processor’s records of processing activities may be shared with the controller" (emphasis ours). The EDPB does go on to say, however, that "such information should include information on the functioning of the systems used, security measures, retention of data, data location, transfers of data, access to data and recipients of data, sub-processors used, etc.", showing that the amount of information to be made available can be fairly important.

  On audits, the EDPB's guidance is surprisingly limited, only stating that the parties "should cooperate in good faith and assess whether and when there is a need to perform audits on the processor’s premises". The EDPB does not address practical questions that controllers and processors have faced regarding the frequency of audits, the possibility of joint audits (on behalf of several controllers, to limit disruption for processors), the possibility for the processor to provide reports of audits carried out on its own behalf (several processors exclude the possibility for controllers to carry out an audit on their own initiative and force them to accept reports drawn up by auditors appointed by the processor), etc. In this respect, therefore, the EDPB guidance is in our view not likely to change the clauses that are commonplace today.

What about liability?

Given the extensive input given by the EDPB on all of these requirements, it appears surprising that the issue of liability barely features in these controller-processor guidelines. Article 82 GDPR contains various rules on liability between controller and processor and on liability of controllers and processors vis-à-vis data subjects, but the EDPB does not mention that provision of the GDPR, likely because it is composed of supervisory authorities (not courts or lawyers). However, it is crucial to bear liability in mind when negotiating and reviewing data processing agreements.

In other words, do not expect to see in this guidance any suggestions on the strategic choices to be made (going for unlimited or capped liability, which types of damage or loss to cover, etc.), but avoid using the EDPB's guidance as a comprehensive checklist precisely for that reason. For that, you will still need to determine your own strategy.

Don't agree with the guidance? Submit feedback to the EDPB

These controller-processor guidelines have been published online in the context of a public consultation that runs until 19 October 2020.

As a result, if you feel as though these guidelines are too far-reaching or impose excessive requirements, there is always the option of voicing your concerns. Bear in mind that comments might be published on the EDPB website, so companies may wish to get in touch with peers and submit a sector-wide response, to avoid drawing too much attention to them individually.

In any event, these guidelines should prompt you to look over your data processing agreements. Do get in touch – it will be crucial to check whether all of the EDPB's concerns and recommendations are already taken into account; if not, it might be necessary to adapt your agreements in the light of this new guidance.