VLP LAW GROUP LLP

Top Five Pain Points in Data Processing Agreements - a Blog Post by Michael Whitener

Drafting a GDPR-compliant data processing agreement (DPA) should be dead simple. After all, GDPR Art. 28 provides a specific roadmap of what to include.

Yet DPAs – which are required under the GDPR whenever a processor is processing personal data on behalf of a controller – can sometimes be the tail that wags the dog in commercial agreements. Got the services agreement executed? No sweat. But the DPA? Oops – holding up the transaction.

The problem is that DPA templates, whether provided by a customer (controller) or a service provider (processor), rarely stick to the bare bones of what the GDPR requires. Negotiating various non-essential terms can greatly prolong the path to execution.

Here are the top five pain points when negotiating DPAs, in my experience – along with some compromise tips.

1. Limitation of Liability
This issue isn't addressed at all in GDPR Art. 28 – leaving it to the parties to negotiate.

The easy solution is for the DPA to stay silent on the topic. In that case, assuming the DPA is integrated into the related services agreement, whatever liability terms are agreed in the services agreement will apply to the DPA. Those liability terms may well include a carveout for data protection obligations.

Quite commonly, however, a controller-friendly DPA will state that any liability limits in the services agreement won't apply to the DPA. Conversely, a processor-friendly DPA will state that any liability limits in the services agreement do apply to the DPA, and moreover any claims under the DPA will be aggregated with any claims under the services agreement.

Compromise tip: For clarity, I like to shift any liability terms to the services agreement alone, with liability under the DPA specifically addressed in the services agreement. What is increasingly becoming "market" is for customer and service provider to agree on a "supercap" applicable to breach of data protection obligations, including the DPA – either a multiple of fees paid/payable under the services agreement or a flat dollar (or other currency) amount.

2. Use of Subprocessors
GDPR Art. 28 is oddly opaque on the subject of a processor "engaging" another processor – i.e., a subprocessor.

Authorization to use subprocessors can be either “specific” or “general.” “Specific” authorization is clear enough: the controller must approve each and every subprocessor. “General” authorization, however, come with a requirement that, if the processor intends to add or replace a subprocessor, the processor must inform the controller, “thereby giving the controller the opportunity to object to such changes.”
In the case of general authorizations, typically the DPA will either list out the subprocessors that are being authorized as of the date of the DPA, or else the DPA will provide a link to an online list of subprocessors.

Let’s suppose the controller objects to a new subprocessor. Then what? The GDPR doesn’t tell us, and many DPAs don’t either. At one extreme, the DPA terms say the processor will breach the agreement if it uses a subprocessor over the controller’s objection. At the other extreme, the controller can object, but it’s a toothless objection.

Compromise tip: The “market” solution that has emerged is for the processor to provide notice to the controller of its intent to use a new subprocessor, with a time window (negotiable) within which the controller can object. If the controller does object, and the parties are unable to resolve the objection, the controller’s only remedy is to terminate the agreement. In other words, no single customer (controller) has the power to stop a service provider (processor) from using a particular subprocessor – but the controller is granted exit rights from the relationship.

3. Security Measures

The GDPR’s requirements regarding security measures are addressed in Article 32 (Security of Processing), which are looped into the DPA via GDPR Art. 28. The Article 32 requirements aren’t particularly onerous: requiring “appropriate” technical and organizational security measures, along with several factors to ensure the level of security is “appropriate to the risk.”

The quite flexible GDPR security terms haven’t hindered controllers from trying to impose their own extensive security requirements on processors. Naturally, processors push back against having to comply with a host of customer requirements.

Compromise tip: Processors should be allowed to rely upon their own security standards rather than sift through the requirements of multiple controllers. At the same time, the processor must be able to demonstrate that it has actually weighed its security measures against the criteria outlined in Article 32.

4. Responding to Data Breaches

The obligations of controllers and processors to provide notification of data breaches are unbalanced in the GDPR. The controller must notify “without undue delay and, where feasible, not later than 72 hours after becoming aware of it.” The processor, on the other hand, only has a “without undue delay” obligation to notify.

Nevertheless, many controllers impose time limits on the processor’s notification to the controller. Language such as “immediately, and in any case within 24 hours” is common. The 24-hour mandate is sometimes justified as being necessary because it gives the controller another 48 hours within its 72-hour window; but that’s a misreading of the 72-hour requirement, since the countdown doesn’t begin until the controller has “become aware” of the breach (i.e., in the case of a processor breach, whenever the processor notifies the controller). Processors, of course, would much prefer to simply rely upon the GDPR's generous "without undue delay" language.

Compromise tip: Although the GDPR doesn't impose any specific time limit on a processor's data breach notification obligation, it's not unreasonable for a controller to impose one. The time limit, however, must be feasible. In my view, 48 hours is the minimum period reasonably required to perform the data breach assessment necessary for a breach notification to be useful – including details on the records accessed, whether the breach has been remedied, etc. And the time period should only begin when the processor actually becomes aware of a true breach; requiring notification of "suspected" breaches isn't necessary or even useful.

5. Audit Rights
GDPR Art. 28 gives the controller certain audit rights to ensure that the processor is complying with its GDPR obligations. The scope of the audit includes "inspections," which isn't defined but is presumed to include facility inspections.

DPA audit provisions can be quite extensive. Controllers sometimes ask for the right to pop in and conduct an audit anytime, and even insist on the right to audit the processor's subprocessors. Processors, on the other hand, want to limit the scope and timing of audits. The limitations that processors propose typically include advance notice, the controller's compliance with the processor's security/confidentiality requirements, and sometimes even reimbursement of the processor's expenses incurred in connection with the controller's audit.

Compromise tip: Since the GDPR's audit provision initially refers to making available "all information necessary to demonstrate compliance," it's reasonable that, as an initial step, the processor is only required to provide any audit or certification documentation (e.g., SOC 2 report, ISO 27001 certification). Only if the documentation is not sufficient should an on-site audit be appropriate. Ultimately a processor can't deny a controller the right to an on-site audit, but it's entirely consistent with the GDPR terms for the DPA to require the parties to agree as to reasonable scope, timing, duration, etc. of the audit.

* * *

Maybe one day the European Commission will resolve these pain points by implementing "standard data processing clauses" along the lines of the current standard contractual clauses, with perhaps a few optional clauses for controller and processor to play with. But don't hold your breath.