Top ten data protection considerations when outsourcing

Molly Waiting, Associate with Bates Wells, offers ten key data protection considerations for controllers considering outsourcing internal functions

It is five minutes to six on Friday night. You are ready to sign off, looking forward to a take-away and *Hamilton* on Disney+ (because, let's face it, that is the best we have right now). Your Chief Operating Officer calls. She informs you that, as part of the cost savings programme in response to the pandemic, the company plans to outsource a number of its internal functions. She asks you what she should look for during the procurement process. By Monday morning, of course. What do you do? Below we have set out ten key considerations from a controller's perspective when thinking about outsourcing.

1. What's involved?

What exactly will the provider do? What types of personal data will the provider have access to? Whose personal data are involved? These questions may seem obvious to ask, but they help determine the data protection risk of the outsourcing and to take a proportionate approach at the outset.

Many contract negotiations go awry because these details were not clarified at the beginning. For example, one company we know insisted upon a 45 page data processing addendum, only to figure out after weeks of tense negotiation (and thousands in legal fees) that the only personal data involved were employee names, email addresses, and job titles. These details will also help determine whether you need to — or should — perform a data protection impact assessment because (for example) the outsourcing involves a particularly innovative technology, like an automated solution which uses AI.

2. What's the relationship?

In most outsourcing scenarios, the provider will act as a processor on behalf of the controller. However, this will not always be the case. Take, for example, outsourcing legal work to an external firm. Lawyers in the UK are subject to separate regulatory obligations and are expected to act with a degree of independence. They are considered controllers of client personal data.

Even the general assumption that providers act as processors is becoming strained. Providers are increasingly more sophisticated in the solutions they provide, which limits the actual amount of control that the controller has over how and why personal data are processed. Moreover, providers often seek to use their clients' personal data for analytics in order to improve their products and services. For example, cloud management platforms will track users' engagement in order to improve the overall user experience. With the increase in AI driven solutions, the line between processor and controller will only become more opaque. The upshot is that controllers should be sure to ask questions and deal with the relationships clearly in any agreement.

3. What due diligence is necessary?

Controllers are required to choose processors that provide sufficient guarantees that they will process personal data safely, securely and in accordance with applicable laws. This can be demonstrated by performing due diligence, and keeping a record of that due diligence.

Ideally, controllers should include due diligence as part of the procurement process (for example, in the Request for Proposal). If they wait until a provider is selected, they run the risk of discovering a significant data protection concern, and either proceeding in the knowledge there's a risk, or having to repeat the procurement exercise (with the associated expense and delay).

Controllers should also refresh their due diligence regularly during the course of the relationship. Many outsourcing arrangements include annual audit programmes; controllers should ensure that data protection compliance is included as part of the audit programme.

What should controllers ask of their outsourcers? This will depend upon what's involved. Due diligence should be proportionate: two or three ques-

(Continued on page 4)

(Continued from page 3)

tions will not be sufficient for a major outsourcing arrangement. On the other hand, a 30 page questionnaire for an email marketing solution is excessive. In general, we recommend:

- asking to see relevant internal policies or the most recent audit report (for example, from their ISO 27001 or SOC 2 certification), with the aim of discovering things such as how they handle reporting breaches;
- establishing the specific security measures that apply to the services being procured and establishing whether these are sufficient;
- if the provider is not based in the UK or the EU, checking whether they are familiar with European data protection law and whether they have other clients based in the EU;
- asking about the systems that will be used. Will these systems be required to integrate with your existing systems? The Information Commissioner's Office found that the failure of Marriott International to perform due diligence into systems integration was a factor in the data security breach still under investigation; and
- finding out whether the provider sub-contracts their services, and if so, to which entities (where are these entities based?)

4. Whose contract?

We all like to use our carefully drafted template data processing agreements, full of controller-friendly provisions. However, in the context of outsourcing, it often makes sense to start negotiations using the provider's data processing provisions. This is because outsourcing providers often have thousands of clients and so operate on the basis of economies of scale. Given that they rely on using standard data protection provisions for all clients, it would be technically unworkable and financially unviable for providers to agree multiple distinct data processing agreements, each with slightly different reporting times and audit rights. Insisting on your own data processing agreement can mean that you enter into extended negotiations with the provider. Some providers even increase their fees for bespoke data processing arrangements.

"We all like to use our carefully drafted template data processing agreements, full of controller-friendly provisions. However, in the context of outsourcing, it often makes sense to start negotiations using the provider's data processing provisions."

If the provider's data protection provisions don't comply with the requirements of Article 28 of the GDPR (which sets out the requirements for the controller/processor relationship), then you should request compliant provisions or revisit their due diligence and risk appetite. A poor contract suggests the provider may not understand their obligations under data protection law.

5. Where's the personal data going?

Many providers are based outside Europe (or use group companies based outside Europe), where the costs of business are reduced (for example, lower wages and limited regulatory compliance). Controllers must find out not only where the provider is based, but also where its group companies and subcontractors are based if they are involved in providing the outsourced services.

As outsourcing companies often work in low-regulatory jurisdictions, there is unlikely to be an adequacy decision (although many US providers rely on Privacy Shield). Binding Corporate Rules remain quite rare, as well. And so the controller is likely going to need the Standard Contractual Clauses. Despite what some may argue, derogations under Article 49 are unlikely to apply because the transfers of personal data in outsourcing arrangements are usually repetitive.

The important point is to make sure that if you are a UK based controller (for example), you have in place a mechanism which allows you to transfer personal data outside the UK or EEA, and that this mechanism covers all personal data (and all parties who will receive the personal data).

6. Are there hidden costs?

If starting from the provider's data processing provisions, controllers should look out for hidden costs. For example, many provider-friendly data processing agreements will include the ability for the provider to charge for additional security measures to those outlined in the proposal; assistance with data protection impact assessments; and assistance with responding to individual requests

On the one hand, you could argue that these are all legal obligations on the provider under Article 28 and should be included in the service free of charge. On the other hand, providers have often costed their outsourcing solutions with a relatively low margin, and so providers risk reducing their profits if they agree to provide all of the above free of charge. If controllers cannot avoid these additional costs, then they should at least ask for clarification about when they will apply and the rates at which they will be charged.

7. Will they use sub-processors?

Providers often rely on a network of group companies or third parties to provide the services. Controllers need to consider how much control they wish to have over the provider's subcontracting, and whether that control is administratively workable. For example, if controllers require providers to seek consent for any new sub-processor, then they need to make

sure that they have the capacity and resources to respond to such requests reasonably quickly.

If controllers instead give the provider a general authorisation to use sub-processors, they should consider:

- how the provider will give notice. Some providers will simply update a list of sub-processors on their website and expect controllers to check periodically;
- whether to request any due diligence on the sub-processor from the provider. For example, a summary of the proposed security measures and a copy of the contract;
- the timeline in which controllers can raise objections to the sub-processor. This needs to be balanced between the response time of the controller's business and the operational needs of the provider (for example, a provider often will not be able to wait 2-3 months to enter into a contract);
- what is a reasonable objection? Should the controller's objections be limited to data protection risks, or include reputational risks; and
- what happens if controllers object? Do they try to agree a workaround? Can they terminate the agreement? Are there any early termination charges that will apply?

8. What happens when things go wrong?

Lawyers and data protection professionals are always accused of planning for the worst. And this is true, to a certain extent. However, data security breaches can place a huge amount of stress on a controller's relationship with its provider. And so it is helpful to have clear expectations on each party included in the agreement. For example:

- include a deadline for initial reporting of suspected breaches to the controller. Depending upon the importance of the services and the sensitivity and volume of the personal data involved, this usually ranges between 12 to 72 hours after the provider becomes aware;
- include an ongoing obligation to provide information to the controller during the course of any investigation;
- make sure the data processing provisions and liability provisions work together. It's great to have a separate data protection indemnity, but that will mean little if that indemnity is subject to a low cap on overall liability; and
- consider more creative solutions. If, for example, the personal data involved will include information which poses a risk of identity theft if accessed, the controller could include an obligation on the provider to pay for credit monitoring for all affected individuals for a defined period.

9. How do we work together?

Successful long-term outsourcing relationships have clear governance structures, which are usually outlined in the agreement or otherwise recorded in working documents. From a data protection perspective this should include:

- appointing a data protection lead for each party. This should be an individual with sufficient knowledge and authority to take decisions;
- regular review meetings where the data protection leads discuss any issues, additional services, changes in law and updates to the agreement; and
- including data protection compliance in the audit programme. Or, if a controller does not have the resources to conduct its own audits, making sure the provider is independently audited and the controller has access to the reports.

10. How do we end the relationship?

Ending an outsourcing relationship can be more complex than simply providing a few months' notice in writing, and instructing the provider to return or delete personal data.

Outsourcing contracts often include detailed exit planning provisions which allow for the gradual wind-down of services. The purpose is to allow controllers to either bring the services in house or transfer the services to a new provider. So, instead of including the boilerplate return/delete clause at the end of data processing provisions, consider how these will work with any exit plans. For example:

- the format for the return of data is incredibly important. Providers sometimes use proprietary databases and information management software, and so controllers need to make sure that they have access to personal data in a form which is useful;
- if the services will tail off over time, can the controller do a staged return of personal data, returning/ deleting segments of personal data as the services come to an end;
- an obligation on the provider to work with the controller (and any new provider) to make sure that the systems are compatible, so that the data transfers smoothly;
- the back-up practices of the provider. Back-ups are a business continuity necessity and it is unrealistic to expect providers to be able to delete data automatically from overall back-ups. Therefore, controllers need to know how long data will remain in the provider's systems, and what protections are in place for this period (for example, access restrictions). The data processing provisions should continue to apply for the duration of the back-up period.

This list is not complete. Nor will each consideration be equally relevant in all circumstances. The purpose of this list is to prompt you into asking the right questions (both internally and externally). And hopefully it will help you respond confidently to your COO on Monday morning, without having to do a weekend of work.

Molly Waiting
Bates Wells
m.waiting@bateswells.co.uk