GDPR puts vendor contracts in the security spotlight


David Brook

David Brook, Turnstone Services

The EU's General Data Protection Regulation (GDPR), which is about to come into force, requires the contracts between an IT department and its suppliers to be reviewed and updated.[1] However, successful contract reviews can bring broader benefits – and to IT security in particular.

In the spotlight

The GDPR programmes that companies currently have in motion are bringing IT vendor contracts into the spotlight. The GDPR changes the regulations surrounding the retention and availability of personal data in IT systems and as the IT ecosystem of a typical business is typically so interlinked with its chosen vendors and service providers, a rethink of the contractual relationships between an IT department and its suppliers is needed. This is to ensure that the processes provided by the third parties are also compliant with the new rulings.

The contract renegotiations associated with the GDPR are closely focused on data security. This article considers a broader review and analysis of vendor contracts and highlights some of the areas where IT vendor contracts tend to be deficient. Eight of the areas we look at impact on IT security. A forensic look at contract terms and a successful review can tighten up these security vulnerabilities and in some cases even make cost savings at the same time. The article concludes by suggesting a strategy for contract review and how companies should focus their attention and renegotiation efforts.

Tighter policy

One of the outcomes of a corporate GDPR programme is that each contract term relating to data security can be clarified and strengthened as part of a tighter, more comprehensive IT security policy.

Reviewing IT vendor contracts is the last step in the process – it logically follows after the earlier stages of a typical corporate GDPR programme:

- Readiness assessment.
- GDPR working group.
- Data inventory.
- Privacy impact assessment.
- Training and awareness.
- Data protection officer appointment.
- Policies and procedures.
- IT vendor contracts renegotiation.

It is at this last stage of the journey, when vendor contracts have been reviewed and updated, that the new GDPR compliant agreements are cemented in place to ensure that the correct services are provided by subcontractors and their contractors.

Red, amber and green

This article examines the findings of a detailed study of 25 real-life vendor contracts that were assessed by CIPS-qualified procurement professionals, rating their completeness and acceptability from the point of view of the customer.

The vendors and suppliers in the review represented various classes of IT vendor: software, datacentre, software support and maintenance, services, telco, hosting, professional services agreements, ICT outsourcing, online cloud services for software as a service (SaaS) and fully managed infrastructure.

In the analysis, the terms of each contract were benchmarked against an established yardstick of what should be present in a fair and equitable contract and were given a simple rating according to how favourable they were to the customer. Where contract terms were acceptable, they were awarded a green light: where they were partly acceptable but deficient in some way they were awarded an amber 'warning' light and where a contract term was seriously deficient or absent – introducing a risk or a business limitation – they were given a red light.

"In the case of 'loss of data', industry best practice requires that the supplier should pay agreed damages for loss or corruption of data. This should be linked to a disaster recovery plan and indemnities"

The analysts studied the contract terms under 27 key headings governing the cost and service areas of the agreement between the vendor (or service provider) and the customer, and compared them to industry best practice.

For example, in the case of 'loss of data', industry best practice requires that the supplier should pay agreed damages for loss or corruption of data. This

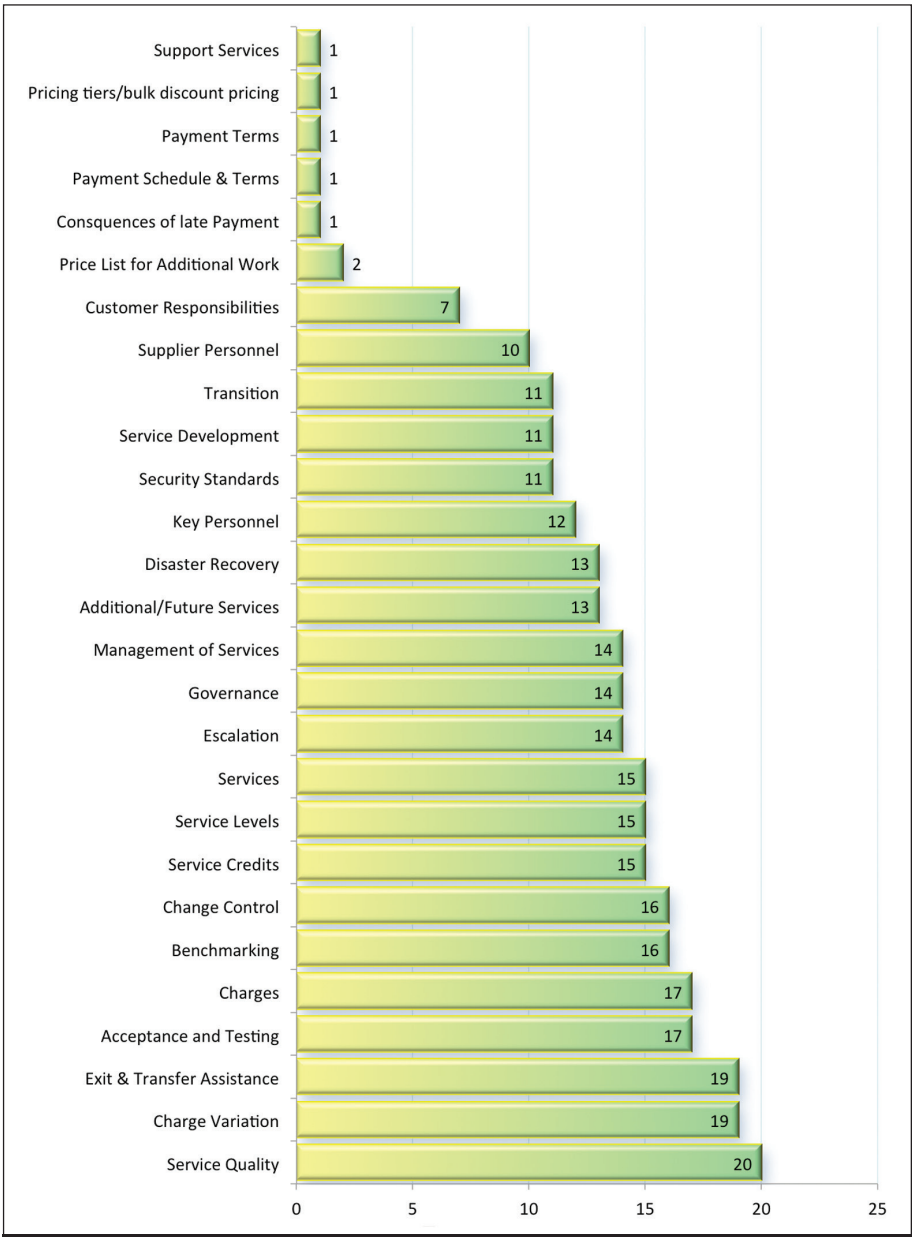

Figure 1: The number of times a contract term was found deficient (awarded a red or amber rating), out of 25 contracts studied.

should be linked to a disaster recovery plan and indemnities. If this point is missing from the contract, the analyst would give the supplier a red light.

Clear picture

The results emerging from the analysis, paint a very clear picture of the contractual areas, including security, that are detrimental to the customer, or unsatisfactory in some way. It's no surprise that suppliers' contracts are worded to suit themselves and it needs more than just a legal resource to identify and then remedy them all.

In the areas that relate most to security – and particularly where contracts relate to subcontractors and their contractors – there were amber warning lights in an alarming number of the contracts studied, particularly in service areas. As can be seen in Figure 1, 50% of the contracts failed to meet best practice for security standards and a worrying 91% lacked detail on service quality. Some of the more general contractual findings were as follows:

Under the heading of 'acceptance and testing', 64% of contracts were deemed to be unacceptable and this heading received the most red lights. Some 77% of the contracts studied were deficient in this area. Services, service quality and service levels also stood out as critical areas where supplier contracts favoured the vendor to an unreasonable degree.

Regarding the important terms surrounding exit and transfer assistance, vendors' standard contracts typically omitted to adequately state their responsibilities and in a surprising number of vendor contracts, this point is missing completely, yet it is particularly important for the customer that the process to exit a contract is clear. It is never too early to define who does what, when and for how much when the exit process is triggered. Both parties need to know what their respective responsibilities are and these responsibilities should be clarified in the clauses relating to customer and supplier responsibilities. However, this is frequently omitted from service provision contracts.

"IT suppliers are often the weakest link in the chain and have been implicated in over half of data breaches, so those aspects of their contracts that represent security weaknesses or liabilities should be assessed with security in mind"

Clauses on another vital area – benchmarking – are often left out or poorly formed. Depending on the contract type, if benchmarking can be better defined, it may provide cost savings or enhanced confidence in the service being provided.

Software contracts are often lacking clarity for the client in the testing and acceptance terms as well as in the areas of change control and disaster recovery. These are especially important when the software is a mission-critical system.

Contracts relating to fully managed infrastructure services require the services to be performed by the supplier to be listed in detail and without exception.

This is often found not to be the case.

IT suppliers are often the weakest link in the chain and have been implicated in over half of data breaches, so those aspects of their contracts that represent security weaknesses or liabilities should be assessed with security in mind. In particular, this will mean that the clauses that relate to areas such as disaster recovery, security standards, change control, management of services, SLAs and service quality, should be carefully scrutinised to be certain that no responsibilities are overlooked and nothing can slip through the cracks.

Vendor contract review

At the time of writing, the May 25 deadline is fast approaching, so the majority of businesses will be quite far down the GDPR path. The GDPR requires certain points to be covered within the fine print of contracts. While there is a published list of these, they need to be appropriately covered in each in-scope contract.

Many suppliers have template contracts that they use, but often these are not updated. This means that when legislation changes there may be a time lag before the relevant clauses are updated. We have seen this with the Data Protection Act and cloud computing and it is happening again with GDPR – suppliers' standard contracts do not cover it.

External procurement legal experts may open up other points of negotiation, so resource it well. Note that you are also one of many customers in the queue for software suppliers, who are likely to be in negotiations with all their customers on the GDPR.

What is involved in reviewing and renegotiating contracts? An experienced eye scrutinises the vendor contract terms and makes a cool comparison with best practice, and highlights those that are not acceptable. These will be the target areas for renegotiations. It is a fact that every single supplier contract favours the supplier and not the customer, but it is also true that these terms can be identified, discussed and improved, in terms of security, liabilities and commercial terms.

The huge amount of work that businesses are investing in gaining GDPR compliance may well turn out to be beneficial because it pushes businesses to review their contracts. This is an exercise that they would benefit from doing anyway, first to ensure that contract terms are clear and fair, not weighted in favour of the supplier – it takes a handful of work days, spread over a month or so, to then eliminate any security loopholes.

"It is a fact that every single supplier contract favours the supplier and not the customer, but it is also true that these terms can be identified, discussed and improved, in terms of security, liabilities and commercial terms"

Although contract reviews may seem onerous, they usually deliver benefits such as better commercial terms and clearer rights and responsibilities, as well as greater protection for the customer. While the GDPR has been a one-off, every company can benefit from re-visiting their supplier contracts, comparing them to industry best practice, clarifying deliverables and tightening up on the security requirements that need to be met.

About the Author

David Brook is co-founder and a director of Turnstone Services (www.turnstoneservices.com), an IT and procurement consultancy. Since its inception in 2006, the company has addressed over 250 separate vendor contracts, working on behalf of clients within the IT function. The company offers IT vendor contract reviews and renegotiations as a service. Brook's goal is to develop IT procurement as a valued and acknowledged skill in the IT community.

Final analysis

The study of 25 real-life vendor contracts leads to the following conclusions:

- Suppliers have template contracts set up but then never update them.
- Changes in legislation see a lag in suppliers updating the relevant clauses – eg, Data Protection Act, data access (cloud computing), etc.
- Benchmarking is a clause that is often left out or poorly formed. Depending on the contract type, this provides savings or confidence in the service being provided.
- Software contracts are the most poorly formed and lacking in clarity for the client when it comes to testing and acceptance, change control and disaster recovery. This is especially important when the software is bespoke and not out of the box.
- Contracts relating to fully managed infrastructure services require the services to be performed by the supplier in detail and without exception. This is found to be not comprehensive.
- Especially important is how to exit certain types of contract. It's never too early to define who does what and when and for how much.
- Both parties need to know what their respective responsibilities are – who does what and when. Clauses relating to customer and supplier responsibilities will clarify this. These are often left out in service provision contracts.

Reference

1. General Data Protection Regulation (GDPR), home page. Accessed Mar 2018. https://www.eugdpr.org.