The GDPR's impact on the cloud service provider as a processor

Mark Webber, Partner with Fieldfisher (Silicon Valley), examines the impact of the new General Data Protection Regulation on cloud service providers

With new requirements for organisations and new rights for individuals, there is no doubt that the EU's General Data Protection Regulation ('GDPR') will have a significant impact on cloud service providers that process personal data ('CSP processors').

Many CSP processors will need to understand their obligations under the GDPR and adapt and amend their services, contracts and background processes accordingly. Those that get on top of understanding the importance of compliance and the basis of that compliance will be able to distinguish themselves in the market.

To date, there has been a lot of headline-grabbing generic GDPR coverage: fines, breach notification and enshrining the right to be forgotten into law. As the dust settles, CSP processors must assess what the GDPR means for them. This article looks at the new provisions specifically from the perspective of CSP processors.

Processors can no longer hide

Under the current EU Data Protection Directive (95/46/EC — 'the Directive'), it is data controllers rather than processors that carry the burden of legal compliance. Processors carrying out processing on behalf of the controller — as is the case in the majority of cloud service arrangements — are not directly subject to the Directive's rules.

The GDPR changes that by expanding the scope of application of EU data protection law requirements, recognising the role that processors also play in protecting personal data. Processors are no longer outside of the ambit of the rules.

Until now, many cloud deals have concluded with the data controller failing to adequately exert controls over the data being processed by CSP processors. The latter, particularly those based overseas, have attempted to force their customers (the data controllers) to 'rep and warrant' that they would act in compliance with all local data laws, and that they have all necessary consents from data subjects to pass data to the CSP processors pursuant to the services. This scenario, although a nonsense under EU data protection law, was often successful, as the burden of non-compliance falls solely to the customer as controller.

Aside from the new obligations on data processors discussed below, any person 'who has suffered material or immaterial damage' as a result of an infringement of the GDPR shall have the right to claim compensation from the controller or the processor for any damage suffered. Individuals may only claim damages from the processor where it has not complied with obligations under the GDPR 'specifically directed to processors or acted outside or contrary to lawful instructions of the controller'. There are apportionment mechanisms where multiple parties or both controllers and processors are involved in an infringement.

All of this now means that a processor will be directly accountable to those whose data they process. CSP processors might be particularly affected, as they have a deeper pocket and no direct contractual means to easily limit or control their potential exposure. In addition, every processor is also subject to the much-publicised GDPR penal fining regime.

Clearly, under the GDPR it will no longer be possible for CSP processors to position themselves as mere processors and evade the reach of data protection rules. The GDPR requires data processors, including CSP processors, to develop and implement a number of internal procedures and practices to protect personal data. There are some exemptions for SMEs, but the burden on smaller CSP processors should not be overlooked.

Technical and organisational measures

Where processing is to be carried out on behalf of a data controller, the controller shall use only processors that provide 'sufficient guarantees to implement appropriate technical and organisational measures' in such a way that processing will meet the requirements of the GDPR and ensure the rights of the data subject. This immediately sets a high-bar for cloud services, creating a customer obligation to test and examine

(Continued on page 12)

(Continued from page 11)

the solution it is buying.

In addition, taking into account the 'state of the art and the costs of implementation', as well as the 'nature, scope, context and purposes of the processing', both the processor and controller must implement technical and organisational measures to ensure a level of security appropriate to the inherent risks to the data being processed. This may include pseudonymisation or encryption of such data, ensuring confidentiality or an ability to restore the availability and access to data should an incident occur.

These provisions probably entail a need for CSP processors to carry out personalised risk assessments for customers. Conceivably, this risk-based assessment may inform CSP processors of a need to deploy customised protections for different processing scenarios. This will not be straightforward if CSP processors run a multi-tenanted homogenised service.

The adequacy and effectiveness of all solutions should be regularly tested. As a responsibility falling to both controller and processor, such measures are likely to form part of the services offered by a CSP processor. Quality cloud services offer just this sort of protection. However, where generic platforms are provided for the customer to customise, CSP processors may have to take a greater interest in what is processed and how the platform is deployed and utilised by the customer.

Documentation

Earlier drafts of the GDPR required that 'privacy by design' and 'privacy by default' obligations also fall only on the processor. These provisions did not make it into the final text. However, the accountability principle within the GDPR introduces a new record-keeping obligation on data processors.

"If CSPs do just one thing, they should review the bombshells contained in Article 26. Under this Article, 'the processor shall not enlist another processor without the prior specific or general written consent of the controller'."

Internal documentation setting out full details of the various processing activities that data processors undertake, and the types of data processed, will need to be maintained by all entities employing more than 250 persons (and in some limited cases by organisations employing less than 250). CSP processors will need to produce and retain such documentation which is to be made available to any requesting Supervisory Authority. This new burden is likely to focus the minds of CSP processors on their potential liability for data put into the cloud.

Under the current Directive, and particularly in the Infrastructure as a Service ('IaaS') or Platform as a service ('PaaS') context, CSP processors were not required to be particularly interested in the data they were processing.

Now, with an (albeit basic) responsibility to understand and log processing, this may lead to more debate about the risks associated with the data and where that risk should fall out between the contracting parties — particularly when CSP processors merely provide platform infrastructure and the customer is actually responsible for implementing security within it.

In such cases, the respective roles and liabilities will need to be spelt out.

A Data Protection Officer

Central to the GDPR's accountability principle is the requirement for certain organisations to appoint a Data Protection Officer ('DPO').

This DPO requirement may also fall to processors (depending on the nature of their core activities and/or the type of data processed). If required, processors must allow the DPO to act relatively independently and, amongst other things, provide oversight with regard to the risks associated with the processing operations.

(As a brief recap, the GDPR will apply to the processing of personal data by a controller or a processor which is established in the EU. Under certain circumstances, it will also apply to the processing of personal data of data subjects who are in the EU by a controller or a processor which is not established in the EU. This means that the obligation to appoint a DPO may still apply to a processor which is not established in the EU.)

Somewhere along the line, the facilities and processes to effect compliance will need to be funded. It's likely this burden will be pushed down to customers within service fees.

Subcontracting generally

If CSP processors do just one thing, they should review the bombshells contained in Article 26 (note references may change when the final text is published). Under this Article, 'the processor shall not enlist another processor without the prior specific or general written consent of the controller'. In effect, this means transitioning to a regime of sub-contracting only with consent.

There is express acknowledgment in the GDPR that an open consent to subcontract processing can be agreed upfront. Where general consent is attained, CSP processors should always inform the data controller if there are to be any changes, additions or replacement of these sub-processors 'thereby giving the opportunity to the controller to object

to such changes'. All CSP processors are aware that potential obstacles to sub-contracting should ideally be avoided. CSP processors serving thousands will want to reserve flexibility over their operations.

Where a CSP processor enlists another processor in order to carry out specific processing activities on behalf of the controller, it must ensure that it passes on the 'same data protection obligations as set out in the contract' between the controller and CSP processors. In particular, these flow-down obligations should provide sufficient guarantees around security in such a way that the processing will meet the requirements of the GDPR. Where the CSP's sub-contractor fails to fulfil its obligations, CSP processors remain fully liable to the customer for the acts of their subcontractor. Although this is not unusual as a contractual requirement, the practicalities make the mind boggle. The obligation is to pass through the 'same' terms as the underlying contract — not simply 'substantially similar' terms.

Practically, if CSP processors do not contract on an identical form with every customer, they should be passing down the alternative terms agreed with each respective customer to each sub-contractor processing their data. This will clearly be impossible for large CSP processors with numerous customers and a myriad of subcontractors (not least where backend hosting services are provided by the likes of Amazon or Microsoft).

Ultimately, some of the contractual risk is likely to be absorbed by CSP processors. Ignoring the issues surrounding data transfers outside of the EEA — which will continue in a similar vein to provide contractual discomfort — this particular sub-contracting requirement is likely to plague many legal teams.

Impact on cloud contracting

Processing carried out by CSP processors shall be governed by a contract which binds the processor to the controller, and sets out:

- the subject-matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subjects; and
- the obligations and rights of the controller.

The contract must also stipulate that the processor shall:

- process the personal data only on documented instructions from the controller (including with regard to transfers of personal data to a third country or an international organisation);
- ensure confidentiality; and
- take appropriate measures to ensure security (see above).

The GDPR is prescriptive about the contents of the contract appointing CSP processors. The new rules will require (taking into account the nature of the processing) that data processors assist the controller insofar as this is possible, for the 'fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights'.

These new responsibilities are not necessarily revolutionary, as most good processing clauses today already require co-operation around regulatory or data subject access requests.

However, in addition to this responsibility, at the election of the controller, CSP processors must delete or return all the personal data processed within the cloud to the controller at the end of the data processing services. They must also delete existing copies unless applicable Member State law requires storage of the data.

Breach notification

Under the GDPR, the need for incident response and incident preparedness training within CSP processors will be elevated.

Away from telecommunication service providers, the EU has not seen breach notification requirements for CSP processors until now.

Sophisticated customers have required breach notification contractually for some time, but CSP processors will now find the GDPR requires them to report any data breach to the controller without 'undue delay' after becoming 'aware' of breach. What amounted to good contractual practice now has a legal mandate.

Codes of conduct and certifications

The GDPR allows CSP processors to demonstrate compliance with many of its requirements (including the security and general processor obligations) by either:

- adopting approved 'Codes of Conduct' (think of the long-awaited Data Protection Code of Conduct for Cloud Service Providers still awaiting sign-off from the Article 29 Working Party); and/or
- participating in certification or seal programmes that are approved by Supervisory Authorities (e.g. possibly the TRUSTe enterprise privacy certification or in the UK, a Privacy Seal).

These compliance steps will also be useful to controllers evaluating and assessing processing services as a part of their mandated data protection impact assessments.

CSP processors will need to wait to see what codes of conduct or certification mechanisms evolve and attain approval in order to determine whether adherence could make sense to them. Certification is certainly worth considering if it allows some form of defence from aggressive regulatory scrutiny and distinguishes CSPs from their peers.

Accommodating the needs of the controller

The majority of obligations under the GDPR still fall upon the controller. Despite that, it may well fall to the CSP processors to adapt infrastructure or services to accommodate the service and legal burden of their customers.

(Continued on page 14)

(Continued from page 13)

Data subjects have enjoyed a right to rectify 'inaccurate' data under the Directive and this will continue. The GDPR now introduces the 'right to be forgotten'. Under this new right, the data subject shall have the right to require the controller erase personal data concerning them 'without undue delay' and the controller shall have the obligation to erase such personal when particular grounds apply. The GDPR also introduces an obligation of data portability — that the data subject shall have the right to receive their personal data from a controller for example so they may move it to an alternative service.

All of these rights are exercisable against the controller, not the processor. However, they may create obligations that the controller requires the more technically proficient CSP processors to facilitate. Erasing, altering or moving all data from a complex technology infrastructure is no simple thing — not least where distributed storage or computing facilities are deployed. Additionally, with the definition of personal data extending in scope to unique identifiers such as MAC, IP, UDIDs and others user specific IDs, more and more datasets may need tracing in order to meet these obligations.

Compliance could come earlier than you think

The GDPR is not yet binding law, and at the time of writing, we're more than two years from it becoming actual law.

Yet, as service providers, the majority of CSP processors are always responding to the needs and wants of their customers. Those CSP processors entering into longer term or rolling contracts with savvy customers will want their contracts to reflect the incoming law. A proper understanding of the GDPR's requirements will help a CSP processor to distinguish the over-enthusiastic customer request from legal requirement, and to ensure fair apportionment of obligations and liability.

One potential pitfall of the new rules is that the GDPR is drafted with the binary assumptions that there are only controllers or processors. The realities of many cloud ecosystems are that there are groups of companies buying services, sometimes through resellers for CSP processors with operations and hosting facilities scattered and sometimes subcontracted across the globe.

Finally, the novelty and uncertainty of the new rules, plus the consequences of non-compliance, will do much to elevate the attention paid to data protection clauses in cloud contracts.

Mark Webber
Fieldfisher
mark.webber@fieldfisher.com