ECIS panel event: GDPR ONE YEAR ON

Data privacy and security in the cloud: where are we?

12 June 2019

One year after the implementation of the General Data Protection Regulation ("GDPR"), some of the text's provisions are still hotly debated. What are the requirements we have seen cloud providers struggling with? Have some of the mechanisms of the GDPR failed to deliver all of their promises? On which requirements have DPAs focused their enforcement actions so far? And looking to the future, what appear to be the emerging privacy trends and challenges? The event had a particular focus on data privacy and security in the cloud. Our panel of speakers included industry professionals and below are summaries for each of their presentations and findings.

Jonathan Sage

Chair of ECIS Public Affairs Group and IBM Government and Regulatory Affairs

We are a year down the road with GDPR. From a cloud perspective, we are seeing a lot of activity at a European level related to security and privacy not only with GDPR, but also with the NIS Directive, the newly implemented Cybersecurity Act, and quasi-regulatory measures, examples of codes of conduct such as the EU Cloud Code of Conduct under Art 41 of GDPR and under Art 6 of the Regulation on the free flow of non-personal data which deals with cloud switching and data portability. Also, the Commission has recently released its Cloud Strategy. Effective for the next four years, it represents the Commission's internal cloud strategy and approach to digital transformation, and explores the multi-jurisdictional effects of GDPR on the Cloud Act. It is suggested that with the right checks, scrutiny, and technical controls, the residual risks are acceptable for us to nevertheless attempt to boldly break out and benefit from new cloud offerings. The Commission argues that it needs to be able to use "best of breed", Cloud solutions, particularly in the Software as a Service area and deploy a multi-cloud, hybrid cloud environment, otherwise they cannot benefit from the digital transformation that they aspire to and risk being locked into one or two cloud providers.

Mark Watts

Partner at Bristows with expertise in Machine Learning and Cloud Computing

The first thing we learnt since the implementation of GDPR is that the world did not end. It was feared that GDPR would be disastrous for businesses, but on 25 May 2018, it felt like business as usual, with many initially questioning whether GDPR was just a lot of fuss over nothing given that there appeared to be no immediate enforcement. There are, however, better metrics (other than the amount of enforcement and the number of fines issued) by which to assess the effectiveness of GDPR. Rather, better metrics include the analysis of: how many companies have since developed suitable data protection programmes; how many CEOs and boards have since become engaged with the issue of data protection; or how many individuals have since been made aware of their exercisable fundamental rights?

Companies have started to take the notification obligations of their data breaches very seriously. This has led to a lot of "borderline" notifications in circumstances where there is most likely no risk to data subjects, but where companies will notify just in case, so as to avoid potential action or criticism from the regulators. However, the regulators (for example in the UK) are discouraging companies from making borderline notifications, as their time is not best spent dealing with companies trying to "clear their conscience". Their time would be better spent addressing incidents where there is an acute risk to individuals' data. We expect to see regulators clamp down on this further, hopefully resulting in the stabilising of notifications.

Enforcement has kicked off and companies are being fined. Around 12 Member State regulators have issued fines, including CNIL's eye-catching 50 million euro fine imposed on Google France. However, often these cases turn exclusively on their own facts and one should not extrapolate too far that they might meet a similar end. There has also been a rise in class actions brought against security issues affecting large swathes of people.

GDPR has become "contagious" and is catching on around the world. For example, the Brazil Act 2018 is closely aligned with GDPR. Needless to say, the territorial and jurisdictional reach of GDPR is so vast that a Brazilian company selling to the EU may be subject to GDPR obligations in any case. Therefore, countries aligning their laws with ours may be a helpful step for all concerned.

A notable success of GDPR is that through the attention and publicity it has generated (causing both understanding and misunderstanding), lawyers have had the opportunity to dispel myths around data to clients.

The finding of "joint control" is also a topic many are increasingly focused on, which is particularly significant for technology companies. For example, if you are running Facebook plug-ins or "like" buttons, or more broadly are collecting data in a collaborative way, it seems, on the basis of some recent cases very likely that you will find joint control. This is troubling many clients at the moment.

Currently on enforcement, a "one-stop-shop" approach does not appear to be working well. There is uncertainty and inconsistency emerging from the DPAs when they receive complaints, as it is not immediately apparent whether one should be the lead authority to handle them or whether they should be delegated to another. This is a work in progress as DPAs muddle through this issue amongst themselves.

In relation to ad-tech, there is still a tremendous amount of ambiguity amongst industry about what the appropriate lawful basis is for the ad-tech ecosystem (including serving cookies, tracking, behavioural advertising). It is unclear whether it should be based on consent or on legitimate interests. It seems that neither approach is optimal, but it is interesting that an industry which plays such an important role in modern day life is in such a place of uncertainty.

On automated decisions, GDPR contains a provision in the ‘data subject rights’ section of GDPR, which is being interpreted by DPAs and some legislators alike, as a prohibition (i.e. not as a right that must be exercised by a data subject to be effective). This is both surprising and unfortunate, particularly as the closest that GDPR comes to imposing an actual prohibition is in relation to automated decision-making involving children’s data. The varying interpretations of "automated decisions" by legislators and regulators is problematic. Where regulators and other countries have imposed a prohibition on all automated decisions, we need to think about what this will mean for artificial intelligence going forward.

Gwendal Le Grand

Director of Technology and Innovation at CNIL, Commission Nationale de l'Informatique et des Libertés, French Data Protection Authority

There has been a lot of publicity surrounding GDPR, and from a regulator's perspective, what we have seen over the past year is that this legislation is working, it is operational, various stakeholders have integrated it and are using it effectively.

Last year, CNIL received over 11,000 data-related complaints (some of which are collective complaints), marking an increase of 32% from the previous year, which means that citizens are increasingly exercising their rights. Many complaints are also "transported", with over 20% of them having an element of formal international cooperation with other authorities in cases where CNIL is not the local authority as it is not a local case, therefore giving each concerned regulator an opportunity to voice its concerns.

On the controller's side, there has also been a huge increase in interactions with the regulator. CNIL's call centre received 190,000 calls last year which is an increase of 22% compared to the previous year.

Equally, CNIL's website had 8 million visits last year, marking an 80% increase compared to the previous year. More and more companies as well as public organisations are now designating a Data Protection Officer.

CNIL's annual report sets out a list of priority areas for 2019. In terms of inspections, CNIL will focus on citizens' rights, on the relationship between the controllers and processers, and the rights of minors. CNIL has also turned its attentions to cloud computing. In 2012, both CNIL and the Article 29 Working Party on Cloud Computing adopted recommendations including standard contractual clauses that service providers could integrate in their contracts, or that customers would expect to find in their cloud services contracts. Since 2012, we see more and more companies moving to cloud. There is an increased systemic risk because most organisations use the same (very big) cloud service providers, each hosting services for numerous data controllers pursuant to contracts, the terms of which they are generally unwilling to negotiate.

Article 28 of GDPR describes the elements to be included in a contract between a controller and a processor. In addition, when it comes to the services themselves, certain aspects need to be clarified, for instance when encryption is mentioned. For example, do we mean encryption of data when it is transported from my device to the cloud service? Or is it encrypted at rest? In memory? Who can access the information? What can system administrators do? Where is the data located? How are the breaches reported to the controller to ensure that obligations are met? These are all areas that we need to dig into to make sure that we, on the one hand, have up-to-date recommendations for cloud providers and for companies moving to the cloud; and also to understand how the ecosystem is working and whether or not it is operating in full compliance with the relevant new obligations under GDPR.

In the CNIL annual report, six specific areas have been identified as being subject to close monitoring this year: contractual clauses between controllers and processors, the impact of EU legislation (such as the Cloud Act), encryption, termination of the contract (how plausible (technically and contractually) is it for someone to take their data back and give it to another cloud service provider?), information on the location of data (given the GDPR focus on the EU's free flow of data and restrictions on data transfers), and breach notifications.

Chris Hutchins
Managing Director for Public Policy EMEA at McAfee

McAfee's latest mission is to secure cloud adoption, to ensure security between and amongst cloud environments, with infrastructure-as-a-service (iaas), software-as-a-service (saas) and the multi-cloud environment in general. This is because digital transformation is leading businesses, enterprises, government and consumers, to run their services in a multi-cloud hybrid environment. The first interesting observation to note on GDPR is that it took an interventionist approach to security management and information governance management. This is in contrast to the previous Directive 95/46 which had only one article on security, whereas in GDPR there are ten operative security management, privacy-related obligations. This forces organisations to invest in technological controls, to manage data security, and to manage privacy. Some of the security-specific obligations we see in GDPR include data breach notification, data mapping, how to manage data privacy risk associated with the cloud, and what to do in the event of a data breach.

Fundamentally, GDPR recognises that security and privacy are wedded together, they are not separate concerns but they are interdependent. McAfee very much supports this approach of a culture of security created by GDPR and believes that there are a range of different legal and software solutions out there which will enable companies to become increasingly compliant. While still in the early days, we see growing market maturity around data loss and around data breach notification, and we see a much stronger recognition of consumers' rights in this area. Companies are much more aware of the financial implications of data loss and the power of misuse of personal information.

The privacy by design and the privacy by default obligations under Article 25 of GDPR are working well at the moment, and represent a positive step change, as trying to introduce fixes to software *after* an incident is a sub-optimal approach. However, we still see challenges around organisations' data visibility. We have commissioned research showing that most organisations think that their employees are using around 30 cloud services where, in truth, the number reaches 1935 in an average-sized organisation. There is thus a distinct lack of visibility of the cloud service environment which presents risks for every organisation and every data controller.

There is also a growing problem with the shadow cloud or shadow IT services environment. Companies simply do not know all the different cloud services that their customers and their employees are using. This is a problem if we want to improve enforcement and implementation because you cannot implement the right policies if you do not have full visibility of the cloud environment. Without this visibility, GDPR compliance may remain out of touch for many organisations.

One area where the co-regulatory approach under GDPR has worked very well in furthering the cloud services option, is the EU Cloud Code of Conduct. As a result, cloud services providers are now in a position to offer more warranties for compliance. This is a positive development as it allows smaller and medium sized enterprises to be better represented and their rights to be better enforced. Major cloud service providers are now much more willing to represent and to warrant data privacy compliance on behalf of their controllers.

Around privacy by design and privacy by default, there is an ongoing challenge in organisations offering cloud services that, despite extensive internal compliance and training efforts, some engineers still do not think about privacy by design at the outset. This is a problem that must be addressed. Whilst it is tempting for enterprises to address on simpler compliance fixes such as ensuring records of processing and robust data-processing agreements it is important that implementing data minimisation practices and data privacy by default programmes are undertaken as a matter of priority. n enforcement, we should not rush to judge the actions of the regulators. Appropriate amounts of time should be dedicated to these complex investigations. We are pleased to see that some outlying countries around data privacy standards, for example Poland, are much more integrated now and are working more actively to meet the norms set by GDPR.

* * *