Cloud Compliance Specialists: Building Bridges Between IT and Regulation and Bringing Data Privacy to the Cloud

Written by Joshua Bucheli, Talent Community Manager at cyberunity, in collaboration with Aljaz Galof, Senior Risk and Compliance Manager and Data Protection Officer at Aveniq, and Peter Kosel, Founder of cyberunity

In 2017 an influential Economist article noted that "data is the new oil" – that is to say that this digital commodity has become the cornerstone of our modern economy. With this poignant analogy in mind, it comes as no surprise that protecting data is a key concern for modern businesses and governance bodies alike.

When thought of as a corporate asset, data is protected predominantly through cybersecurity. Personal data, on the other hand, is subject to data protection considerations – a body of legal and regulatory standards which aims to prevent misuse of our personal data and to protect our personal rights.

However, as the cloud continues to solidify its position as the world's dominant data storage solution, new challenges are arising for both cybersecurity and data protection – challenges that represent new opportunities for specialists who can bridge the gap between such regulations and the cloud.

Where Does Cloud Compliance Stand Today?

"Nowadays, if you are online, whether as a private individual, an employee, or as a corporation, you pretty much always have at least one foot in the cloud", says Aljaz Galof, Senior Risk and Compliance Manager and DPO at Aveniq.

In 2015, 30% of all corporate data was stored in the cloud and that number has since risen steadily. With as much as 60% of data in the business world being stored offsite as of 2022, the cloud has unequivocally become the dominant solution for anyone trying to reduce the costs and increase the efficiency of their data storage. What's more says Aljaz, "because

businesses often integrate their on-premise- and cloud-based data processes, the distinction between the two is beginning to fade".

This begs the question - are issues of compliance being taken into consideration from the get-go in this mass digital migration, or are businesses simply jumping on the bandwagon and dealing with the associated risks after the fact – if at all?

Storing and processing data, especially personal data, comes with certain clearly defined duties and responsibilities – these duties and responsibilities are codified in data protection regulations like the GDPR, HIPAA, or the FADP, to name a few. Abiding by such regulations is no small task and when data storage is outsourced to third party cloud providers, a whole new layer of complexity is added to the mix.

To a large extent, the problem lies in the fact that the use of cloud services falls under 'processing by third parties' (i.e., outsourcing of data processing) according to existing data protection regulations. As such, there are no cloud-specific regulations per se, limiting the guidance available on how to achieve compliance. This is especially true when it comes to cross-border cloud use and the technical and organisational measures that this entails. This lack of pragmatic guidance combined with the (technical) complexity of effective data privacy has led many businesses to take a rather negative view of the cloud, opting for a 'can't be done for reasons of compliance' attitude or sometimes even a 'let's just hope for the best' mentality in terms of cloud compliance.

Businesses who want to take advantage of the benefits of cloud services (even something as innocuous as Office 365) while remaining compliant with data privacy standards need to be able to ensure the protection of personal data throughout the data life-cycle – they need to keep tabs on the kinds of data that are being stored and processed, where this storage and processing is occurring, who has access to said data at different stages in its chain of custody, and so on. This is a tall order, and even if all these things are accounted for, the lack of transparency on the part of cloud providers means that compliance is still not guaranteed. As a result, "although such questions are absolutely key, all too often, they are not brought up at all", says Aljaz.

Beyond the difficulties associated with data protection law in particular, there are also the challenges posed by the outsourcing of business processes in general – something that is especially true when it comes to data security. As we saw in our article on The Data Sentinels of Tomorrow: Cloud Security Specialists, outsourcing data storage comes with the trade-off of giving up control of how said digital assets are insulated against ever increasing outside threats. In the case of data privacy, a similar question arises: how do I make sure that the privacy of the data I am responsible for remains intact if I am not the one who is 'holding' said data? Especially in the case of highly sensitive or confidential data (e.g., patient or bank customer data), ensuring that this data is protected (both in the sense of privacy and security) is crucial.

Finally, the question outsourcing data storage becomes even more critical when it involves handing said data off to an entity in a jurisdiction with less stringent data privacy regulations. Such cross-border outsourcing of data storage, if it is permitted at all, requires added assessments of associated data protection and supervisory risks along with the implementation of myriad additional contractual, organisational, and technical measures. Ultimately, what each of these scenarios demonstrates is the growing need for compliance specialists who can liaise between the theoretical world of regulations and the practical world of data processing on behalf of cloud providers and their clients alike.

Where is Cloud Compliance Headed?
In terms of the general direction in which the field of cloud compliance will develop there seem to be three major options. The first is that governance bodies will draft new frameworks that comprehensively set out how data privacy should be ensured in the cloud (see for instance the EDPB's recent effort). Option 2 is that existing regulations will be amended so as to extend their scope to include provisions specific to data privacy in the cloud. The third option, which Aljaz sees as the most likely, is that regulators and monitoring bodies will provide more guidance on how to apply existing regulations to the cloud.

Beyond this general trajectory however, there are several other key issues within the realm of cloud compliance that remain undetermined – issues which future cloud compliance specialists will have an active hand in steering. This includes, in particular, the aforementioned issue of outsourcing data storage to foreign jurisdictions, or potential data access by security authorities. Interesting questions arise here with regards to the use of seamless encryption techniques that do not jeopardise the advantages of the cloud. Also interesting is the introduction of "data boundaries" by certain cloud providers (e.g. Microsoft's EU Data Boundary) which are intended to strengthen trust in cloud services. Finally, in a context like cloud or data governance where internationally consistent standards are key, questions of digital independence or sovereignty (see Russia or China's plans to develop their own internets) are also coming to the fore.

Cloud Compliance Specialists – Hard Skills and Qualifications
As we have seen, cloud compliance exists at the crossroads between the world of tech and the world of governance and regulation. Accordingly, what cloud compliance specialists need to do above all else, is bridge the gap between these two dimensions of data privacy.

First and foremost, a basic understanding of and affinity for the legal foundations of compliance – ideally IT law – is the most fundamental prerequisite for a career in cloud compliance. This isn't to say that such careers are restricted to lawyers or jurists. Rather, as Aljaz points out, "what is important is that aspiring cloud compliance specialists be able communicate at eye level with legal professionals and auditors, deal with contracts, and understand the nuances of the regulations that they are tasked with implementing (e.g., the GDPR)".

Beyond this, they also need to understand the technical aspects related to such regulations. They must be familiar with the kinds of data that are being stored and processed, where this storage and processing is occurring, who has access to said data at different stages in its chain of custody, and so on.

Take the deletion of data for example, a critical issue in the data privacy world. Cloud compliance specialists not only need to be able to refer to regulations and advise on *when* data must be deleted – they must also be familiar with the technical processes involved with said deletion to consult on *how* and monitor *whether* this data has indeed been deleted. After all, in an age where information is predominantly stored virtually (digitally) *and* offsite (in the cloud), an intern with a shredder will no longer suffice for the purging of sensitive information.

Due to the interdisciplinary nature of cloud compliance, it is a field that lends itself well to lateral entrants. "Individuals with experience as legal professionals, computer scientists, IT governance professionals, quality and risk management specialists – anyone who has experience dealing with assurance processes, implementing internal regulations, or carrying out internal Audits will have a good foundation upon which a career in cloud compliance can be built", explains Aljaz.

Degrees, Diplomas, and Certificates:
For now, degree programs that combine the technical and regulatory aspects of data privacy are few and far between, though this seems to be changing slowly in the context of continuing education (see, for example, The University of Applied Sciences in Cologne's LLM in Compliance and Corporate Security, or the CAS Data Privacy Officer at the HSLU, Digital Compliance Officer at the HWZ, and Managing Privacy and Data Security at the USG). Until such programs become more accessible at the degree level, a university education in computer science or business informatics coupled with practical IT experience will offer the best foundation for aspiring cloud compliance professionals.

Cloud compliance is both an interdisciplinary and a nascent discipline. As we have already seen, it requires the shared skills and experience of legal professionals and IT specialists, a combination that is not yet well represented in educational programs. As such, cloud compliance remains a field that requires teams of multiple individuals with multiple skillsets and backgrounds.

In terms of professional certifications, Aljaz recommends a combination of certificates that offer a basic understanding of the inner workings of cloud platforms on the one hand and of information security on the other. Programs like Microsoft Certified Azure Fundamentals, Google Cloud's Foundational Certification, and AWS' Cloud Practitioner course are a good first step for professionals hoping to get into the cloud compliance field. These are especially beneficial when supplemented by technical certifications like IAPP's CIPP/E or CIPM programs or ISACA's CISM or CRISC.

For those looking to gain an extra edge over the competition, practically oriented data privacy certifications like ISACA's CDPSE are also strongly worth considering.

Personality - Beyond Technical Know-How:
Apart from being able to speak the languages of both IT and legal professionals, successful cloud compliance specialists will also bring with them a particular set of personality traits. For example, "they will need to be able to maintain a big picture perspective while dealing in a field where it is easy to get caught up in the details", says Aljaz.

Ensuring data privacy when dealing with cloud storage solutions is a complex process that is yet to be clearly defined and which still has a lot to do with assessing and then taking calculated risks. As such, it takes someone with a considerable degree of pragmatism – someone who is comfortable with setting and confidently pursuing a course of action in the face of uncertainty.

Another key characteristic of an effective cloud compliance specialist is an affinity for interdisciplinary teamwork and a knack for diplomatic horizontal and vertical communication. After all, cloud compliance is something that takes the combined efforts of techies, jurists, management level decision makers, and everyday employees, and the ability to mediate effectively between these parties is par for the course.

Taken together it is evident that the field of cloud compliance is one that is largely yet to be defined, says Peter Kosel, founder of cyberunity AG. Two things are for certain, however. Firstly, defining this nascent field will largely be left up to cloud compliance specialists, and secondly, due to its increasing dominance as a data storage solution, the future battle for data privacy will predominantly be waged in the cloud. With this in mind, it is clear that in the near future, it will be those businesses who secure top performers for their cloud compliance teams early on that will play the biggest part in defining the trajectory of cloud compliance and who will stand the best chance of avoiding the penalties associated with data privacy breaches.