

The legal sector and the cloud: when doing it right is a must

Law firms can step into the future with confidence if they carefully ponder a key aspect that should by no means be overlooked in their digital transformation projects

The cloud is ready to onboard the legal world in a big way and early success stories already indicate that the benefits for the sector will be astonishing: law firms and legal professionals will work in an all new and empowering work environment that will allow them to better leverage resources, reduce internal costs and offer enhanced service for less. There is however a hidden pitfall to watch out for at the outset of any digital transformation project, in order to avoid a most dramatic risk further down the line. This is illustrated by Logol, a pioneering Swiss company in the field of artificial intelligence and specialist technology partner of law firms, who helps early movers reap that strong competitive advantage they are looking for in a safe and secure way.

For years, the legal world has been sitting on the fence watching the digital revolution, eyeing the incredible benefits that it promises to deliver, but wary of the security risks that it presumably would bring with it. Granting access to critical client data via the internet and storing highly confidential client documents on a third-party cloud infrastructure rather than in a carefully guarded, on-premises data center is not something any privacy-conscious law firm will consent to light-heartedly.

And yet, today, the legal world is taking the big leap. The technology has proven itself worthy of trust and prime law firms are ready to revolutionize their operational processes and embrace the cloud-computing paradigm, receiving benefits such as anywhere, anytime access to data by authorized users. The change has occurred surprisingly quickly and, more than just a pathway to a healthy competitive advantage, the cloud is now seen as a ‘must-have’ by large parts of the legal world.

Software manufacturers have sensed the change and, with comparable rapidity, have adapted their offering to meet the new demand. Software management systems and applications for the legal world are now all ‘cloud-ready’ and offered via the modern SaaS (software as a service) model. To deliver their services, the software supplier will provide the client not just their applications, but also the cloud infrastructure, either through its own data centers or through those of a third-party cloud provider. In any case, the law firm generally receives a turn-key solution from the software supplier.

While a cloud-based infrastructure model allows law firms to set new standards in terms of effectiveness and efficiency – and should definitely be pursued – there are two issues that must be considered when embarking on this digital transformation journey. Underestimating their pivotal importance can jeopardize business continuity and even survival of the company. And while the first issue is, not surprisingly, security related, the more critical issue is not a data security issue at all!

Compliance and security: the most debated aspects

Traditionally, when software could only be licensed, a law firm would purchase a license and install the product on a server located in their server room or data center. In such a scenario, all security and compliance issues are a responsibility of the law firm.

Today, as the cloud-computing and software as a service (SaaS) model takes hold, law firms no longer need to have an on-premises server room. The software is provided as a service by the software provider, who also supplies the cloud space on which to install and run the applications. In this scenario, the client no longer handles compliance and security issues directly, but must address them to the software supplier. In the case of a law firm, the compliance and security requirements on the cloud are much more stringent than they are in the traditional software license model where servers, software and data are all on the company premises.

While compliance requirements may vary from country to country, law firms will generally need to make sure their cloud provider and software are certified/compliant with GDPR, ISO 27001, ISO 27017, ISO 27018, ISO 22301 and ISO 9001. Often smaller software providers will not be able to provide these types of certifications so the client will only have the certifications of the cloud provider. It is also important to be aware that many vendors have simply adapted software designed for on-premises servers for use on the cloud. These applications are often built with obsolete architectures that feature critical limitations in terms of performance, scalability, compliance and security. Relying on software or a cloud infrastructure that does not meet the highest security standards and the most stringent ISO certifications means running the risk of a data breach, with all the imaginable consequences. Therefore, law firms should make sure their software supplier has the necessary know-how, experience and certifications to meet all the compliance and security requirements that are needed for providing cloud-based services to the legal sector.

Software and data access: a less obvious, but potentially lethal risk

The second issue faced by law firms migrating to the cloud is even more critical and can be illustrated by considering what would happen if the software supplier goes out of business. If a law firm purchases and installs software on their own server and the software company closes, the company can continue to use the software on their system and all their data is safe. The annoying but not disruptive issue faced in this situation is that the software manufacturer no longer provides any software updates and bug fixes, the software eventually becomes obsolete and the law firm will, in the medium term, have to migrate to a new software application and a new provider.

In the cloud model, both the software and data reside on the servers of the software supplier or that of a third-party cloud provider. In the first case, if for any reason the software provider goes out of business and stops paying its utility bills, its servers will get shut down and the law firm will discover from one day to the next that they have lost everything. Their users will no longer be able to access the software and data on the cloud. An unacceptable scenario, both for the law firm and its clients!

One may ask: what if all the data is backed up on an on-premises server – would this solve the problem? Not really: the issue now is how to access the data without the corresponding software. Then what if the client, as a precaution, asks for and obtains a copy of the software from the supplier – would this solve the problem? Once again, the answer is negative. In fact, at this point, the issue is what version of the software will the law firm have when the emergency occurs. Any software solution provided in SaaS mode, if it is a good product, will be continuously upgraded over time. If



the law firm has an old version of the software, say the version installed years earlier when the contract was signed, it may no longer work with the current data structures and could very well be useless for accessing the data, even if it is all backed up on-premises.

An alternative approach, one could think, is to put the software and data on a cloud infrastructure that is not owned by the software provider, but by one of the major third-party cloud providers: Internet giants like Microsoft, Amazon, or, in Switzerland, also Swisscom. While it may seem promising, closer examination shows that the situation does not significantly change. In fact, the moment the software supplier stops paying for the cloud infrastructure, all of its services will be shut down. While the software and data would be intact on the third-party infrastructure, the cloud provider cannot allow the law firm to access it because legally it belongs to the software provider. Moreover, the software vendor's database may contain the data of many clients, making it technically very difficult to extract only the data of one client or to grant a law firm access only to its data and not that of all the other clients. Once again, the law firm would find itself cut off from its software and its data from one day to the next, leaving them unable to operate.

Preserving access to the cloud: Logol's solution

Logol has identified and addressed this less evident issue from the outset. As a pioneering, digital-native consulting firm and manufacturer of comprehensive management solutions for specific market sectors, where cutting-edge technologies can make a phenomenal impact, the company succeeded in setting up an ideal go-to-cloud paradigm for clients in the legal sector that involves a strategic partnership with the cloud provider.

In fact, when signing up new clients for ELLE – it's highly secure, cloud-based law practice management solution which leverages the power of artificial intelligence – Logol prepares not one but two contracts. One is between the law firm and Logol for the delivery of ELLE in SaaS mode and administration of the customer's cloud space. The other is a contract between the law firm and a major third-party cloud provider, in this case Microsoft Cloud, for the cloud space itself and the Microsoft applications. While the customer has only to deal with one counterpart for all matters related to software and cloud services, including payments, the law firm can at any moment decide to step in and manage the relationship with Microsoft for the cloud infrastructure directly. The client will always be able to access the applications and data on its cloud as they retain ownership of this space. Logol is only allowed to administer the space as designated partner.

Caveats and recommendations in a nutshell

In general, when signing contracts with providers of cloud-based software, law firms should make sure that software and data will be hosted by a major third-party cloud provider and that they retain ownership of this space. Thus, should their software provider go out of business, they will continue to have access to their software and data. The law firm can start making payments for the space directly to the cloud provider and inform them that the software supplier is no longer authorized to administer their cloud space. With this arrangement, there are no risks for the law firm's day to day operations. The only issue would be compensation to the software provider for continuing to use their IP that is on the cloud. While this could represent a legal problem, it does not impact business continuity. In the medium term, the law firm will of course have to migrate to a new software solution and provider.



In many countries all over the world, suppliers of software as a service that take care of providing their clients cloud infrastructure from third-parties generally manage the business relationship with the cloud provider directly, retaining all the rights to the cloud space. In Switzerland, where Logol's headquarters are located, the percentage is close to 100%. This is a risky arrangement that law firms should be careful to avoid in order to not risk finding themselves, one day, fighting a battle for survival which they could easily have averted.

About Logol

Logol, Swiss provider of cutting-edge technology solutions, brings the extraordinary benefits of digital transformation and artificial intelligence to the business world. Founded in 2017, the Zug-based company focuses on how the relentless pace of technological innovation is driving market trends. In only four years, Logol has successfully deployed more than 100 projects in a range of key sectors, helping clients to optimize costs, uncover new business opportunities and take their organizations into the future. Rapidly expanding throughout Switzerland and internationally, Logol engages a unique team of 50+ highly qualified and experienced digital-native professionals across its offices in Zurich, Zug, Lausanne (Gland) and Chiasso.

Media contact:

Tim Cockerell
Wise Media AG
Bahnhofstrasse 104
8001 Zurich
Switzerland
T +41 44 536 1685
tim.cockerell@wisemedia.com

Information on Logol:

Julian Deb
Logol AG
Baarerstrasse 14
6300 Zug
Switzerland
T +41 43 268 39 90
info@logol.com