EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of European Lawyers

Rue Joseph II, 40/8 - B-1000 Brussels
+32 (0)2 234 65 10 | ccbe@ccbe.eu | www.ccbe.eu

CCBE guidelines on the use of cloud computing by Bars and lawyers

27/02/2025

Table of contents

I. Introduction

1. Scope of the guidelines

These guidelines aim to create more awareness about various risks associated with using cloud computing in legal practice. The previous version, from 2012, needed updating to reflect the changes in legislation, technological developments and the practice of law. They also aim to give more context to Bars and in the context of their use of cloud services. They are addressed to the CCBE member Bars and Law Societies and are designed to assist in their role of supporting their members.

2. Context

The use of cloud computing and cloud based services has increased in recent years.[1] In the EU, 42.5 % of EU enterprises bought cloud computing services in 2023, mostly for e-mail, storage of files and office software. Compared with 2021, the share of enterprises buying cloud computing services in the EU increased by 4.2 percentage points in 2023.[2]

In 2022, the CCBE ran a survey on the use of cloud computing by lawyers.[3] Although most Bars do not have quantitative information on the use of cloud computing by law firms, many of them reported that such use was on the rise.

In the US, the insights from the 2023 Cloud Computing TechReport of the American Bar Association (ABA) '*reflect a significant increase in lawyers' use of Cloud computing for the practice of law. According to the 2022 Report, Cloud usage increased significantly from 60% to 70%. Solos led the way (increasing from 52% to 84% in one year), followed by small- and medium-sized law firms (roughly 75%, up from roughly 65%).*'[4]

Cloud computing offers numerous advantages, such as more resilient devices and backups and the ability to access data from various locations, and various devices (smartphones, laptops, desktops, tablets, etc.) which is particularly useful for remote and collaborative work. It also provides access to services that may only be available on the cloud[5], along with increased storage space and processing power. Additionally, cloud computing can offer enhanced security solutions and greater flexibility for users. However, collecting, storing, or otherwise processing data in the cloud, especially when it is located abroad, introduces certain risks.

[1] The State of Cloud Computing in Europe and the UK, Kinsta, accessed in January 2024
[2] Eurostat, Enterprises buying cloud computing services, EU, 2021 and 2023
[3] Representatives from 17 delegations answered the CCBE survey: Austria (AT), Croatia (CO), Czechia (CZ), Denmark (DE), Estonia (ES), France (FR), Germany (GE) (answer from the Deutscher Anwaltverein), Greece (GR), Hungary (HU), Ireland (IR), Italy (IT), Liechtenstein (LIE), Lithuania (LIT), Portugal (PO), Spain (SP), Sweden (SW) and the UK.
[4] American Bar association (ABA), 2023 Cloud Computing TechReport, January 2024
[5] For example, translation tools.

3. What is cloud computing?

Cloud computing is a general term for IT infrastructure that involves storing and processing data and software remotely in the cloud provider's data centre or interlinked centres, accessed as a service by using the Internet. It should also be borne in mind that cloud computing nowadays is not just about the storage of data but also about the provision of IT services which run in the cloud, instead of a local server maintained by the user, including lawyers and law firms' personnel (e.g. messaging services for communication with clients, videoconferencing tools, etc.).

According to the US National Institute of Standards and Technology (NIST), cloud computing enables '*ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*.'[6] This definition has largely been followed internationally, most notably by the International Organization for Standardization (ISO)[7] and the European Banking Authority (EBA).[8]

In the EU, however, some of the most recent EU legal acts do not rely on this definition. For example, Article 2 paragraph 6 of the Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC defining "online content-sharing service provider" that is based on the definition of the wider "information society service", and is referring to cloud services (without defining that) as an example of such a service. Similarly, the legal definitions in regulations such the Digital Services Act (or the Platform to Business Regulation (Regulation (EU) 2019/1150) also rely on information society service rather than the less legal, but more technical or everyday term of cloud computing.

Considering these points, these guidelines will not introduce a new or revised definition of cloud computing. Rather than focusing on a specific term, it is more crucial to address the various risks that the use of cloud services can present to lawyers and their clients.

4. How is cloud computing regulated in the EU?

There are number of laws and regulations that affect how business processes can be outsourced to cloud computing service providers. From the perspective of lawyers' professional obligations, the key characteristic of cloud-based services is third-party processing of data, likely including correspondence between lawyers and their clients and other processing of personal data.

At EU level, the protection of confidentiality of lawyer-client communications is recognised as a general principle of EU law by the European Court of Justice and has a legal basis in the EU Charter of Fundamental Rights within its articles 7 on the right to privacy and 47 on the right to a fair trial. If the right to confidential communications with lawyers is not ensured, clients may lack the trust to fully disclose the information necessary for the lawyer to provide accurate legal advice and representation in response to the client's situation. In other words, clients' right to legal advice and a fair trial would be severely undermined.

[6] NIST SP 800-145, The NIST Definition of Cloud Computing, September 2011
[7] ISO/IEC 22123-1:2023(en) Information technology — Cloud computing — Part 1: Vocabulary
[8] EBA Recommendations on Cloud Outsourcing and the forthcoming Guidelines on Outsourcing Arrangements (2018)

In Europe, Article 8 of the European Charter of Fundamental Rights enshrines protection of personal data and Article 6 the right to a fair trial.

The key piece of EU legislation governing the processing of personal data is the General Data Protection Regulation (GDPR)[9], its implementation acts in Member States, and the associated guidance of the European Data Protection Board (EDPB). These, however, do not specifically address lawyers and their obligations but rather have a more general application.

The GDPR sets out legal bases for processing personal data, rights of the data subjects, obligations of data controllers and processors, information security requirements, risk and impact assessments and international data transfers. The majority of obligations rest on so-called 'data controllers'. Lawyers should assume to be the data controller in the context when they're providing legal services or complying with their own regulatory obligations.[10]

Importantly, the requirements for international data transfers, set out in Chapter V of the GDPR, are particularly relevant to cloud services since the latter may be physically based outside of the EU/EEA and thereby trigger numerous obligations for organisations which use such services, including lawyers and law firms. This is because service providers based in jurisdictions outside of the EU/EEA are subject to different regulations and as such they may allow for conduct that would threaten compliance with domestic or European regulations by lawyers and law firms. An important example are the regulations mandating third-country law enforcement and intelligence agencies to access data held by companies subject to their jurisdiction which can impact the confidentiality of the data held by the provider in question.

5. Foreign laws applicable to data

Whenever data is stored or processed in a different jurisdiction than a lawyer's own, there arises a question of which laws apply to it. This is even more important when data is stored outside of the EU/EEA and whether, pursuant to the EU law, the data is afforded equivalent protection to the one applying in the EU/EEA. Lawyers considering cloud computing service providers in the US should take note of the Court of Justice of the EU (CJEU)'s Schrems I and Schrems II judgments involving EU-US data transfer mechanisms. In Schrems II, the Court declared the European Commission's Privacy Shield Decision invalid on account of invasive US surveillance programmes, thereby making transfers of personal data on the basis of the Privacy Shield Decision illegal. Furthermore, the Court stipulated stricter requirements for the transfer of personal data based on standard contract clauses (SCCs).[11] The European Commission has issued an adequacy decision for EU-US transfers of personal data provided that the US data receiver adheres to the Data Privacy Framework - the follow-up to the now rendered defunct Privacy Shield. Accordingly, lawyers relying on service providers in the US are advised to implement a back-up data transfer mechanism through so-called Standard Contractual Clauses (SCC's) – a set of model contract clauses that have been "pre-approved" for adequacy by the European Commission.

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): https://eur-lex.europa.eu/eli/reg/2016/679/oj

[10] European Data Protection Board, 7 July 2021, Guidelines 07/2020 on the concepts of controller processor in the GDPR

[11] For more details on the Schrems II judgment: The CJEU judgment in the Schrems II case, European Parliament Research Service, 2020

6. Broader legal and policy context

In addition, various aspects of cloud services are regulated by several other pieces of legislation:

- Network and Information Systems Directive (NIS2) (2022)[12] (EU-wide legislation on cybersecurity);
- Free Flow of Non-Personal Data Regulation (2018)[13] (aims at removing obstacles to the free movement of non-personal data between different EU countries and IT systems in Europe);
- Cybersecurity Act (2019)[14] (strengthens the EU Agency for cybersecurity (ENISA) and establishes a cybersecurity certification framework for products and services);
- Data Act (2023)[15] (initiative to address the challenges and unleash the opportunities presented by data in the European Union);
- Artificial Intelligence Act (AI Act) (broad legislative framework to govern the provision and deployment of AI systems)
- Cyber Resilience Act (CRA) (another legislative framework focussed on enhancing the cybersecurity of hardware and software products with digital components).

The EU has also set up or facilitated the work of a number of working groups, whose work has defined different voluntary codes of conducts or certification mechanisms. This includes the Cloud Service Level Agreement Standardisation Guidelines (2014) of the Cloud Select Industry Group (C-SIG),[16] or the Switching Cloud Providers and Porting Data working group 7 that defined detailed requirements for exporting and importing data from the cloud when a user wishes to move to a different provider. The examples of some of the codes of conduct include:

- SWIPO SaaS Code of Conduct for data portability for lawyer's own data[17]
- EU Cloud Code of Conduct, cybersecurity and certification schemes (related to the negotiations problems that are not lawyer specific, but common to all SMEs).[18]

7. What are the risks of using cloud computing by lawyers?

The key risk associated with the use of cloud services stems from the fact that the data is processed by a third-party provider who may have outsourced parts of that processing to other

[12] Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L OJ L 333 27.12.2022, p. 80: https://eur-lex.europa.eu/eli/dir/2022/2555

[13] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018, p. 59–68: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807

[14] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15–69: https://eur-lex.europa.eu/eli/reg/2019/881/oj

[15] Regulation (EU) 2023/2854 of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ L 2023/2854, 22.12.2023: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202302854&qid=1717084009218

[16] Cloud Service Level Agreement Standardisation Guidelines: https://digital-strategy.ec.europa.eu/en/news/cloud-service-level-agreement-standardisation-guidelines

[17] https://swipo.eu/saas-sector-group/

[18] https://eucoc.cloud/en/home

third-parties, and which may all be located abroad, including outside of the EU/EEA. This raises questions concerning:

- the lawyer's or law firm's control over their and their clients' data, such as availability of, and access to, data and services provided, maintaining appropriate records of activities in line with regulatory obligations or ensuring the continuity of professional practice and objecting effectively to the processing;
- confidential and privileged nature of data processed and the potential threat to it through loss, theft, and lawful or unlawful disclosure. Especially because a number lawyers' activities are of special interest to malicious actors; and
- how to ensure the accuracy, completeness, and quality of the data outsourced to a multitude of cloud computing service providers and stored over time and in different formats (integrity).

Indeed, among the top three concerns associated with the use of cloud services mentioned by the CCBE members in the 2022 CCBE survey were protection of confidentiality, data control and overall cybersecurity.

These risks may arise in numerous situations and as a result of:

- lack of knowledge of cloud capabilities and technical intricacies (e.g. remote data storage, contractual limitations of some functionalities such as backup and access to data, encryption, etc.);
- lack of understanding of cloud delivery models, including value-added resellers and additional layers of contractual complexity, e.g. long supply chain and multitude of partners used by cloud providers;
- insufficient knowledge of the service provider, namely the financial risk of losing the subscription fees paid in advance and potential loss of data processed by the provider;
- insufficient cybersecurity protections on the user (i.e. the lawyers') side (e.g. insufficient care in maintaining login details for an otherwise secure cloud computing service or use of so-called shadow-IT);
- insufficient knowledge of laws and regulations that apply to data processing and to accessing of data by law enforcement authorities, especially in foreign jurisdictions, or further processing of data by the cloud providers; or
- technical issues and lack of user buy-in related to functionality, usability, or accessibility concerns (e.g. service not having all the required functionality or not being usable to lawyers with a visual impairment);
- lack of understanding of terms and conditions of use due to low transparency from the providers (coupled with the relative ease of use and availability of the solutions);
- failure to thoroughly review the terms of use and associated contractual documentation.

II. CCBE guidelines on the use of cloud computing services by lawyers

National Bars and Law Societies, in advising those of their members who are considering deploying cloud computing in their offices should seek to draw to their attention, among others, the following considerations.

1. Professional obligations

The use of cloud computing services engages several core principles of the legal profession, as set out in the CCBE Charter of core principles of the European legal profession and the CCBE Model Code of Conduct, namely confidentiality and professional competence.

Confidentiality

Lawyers are required to keep confidential their communications with, information received from, and advice given to their clients. The confidentiality of communications between a client and their lawyer is protected by the principle of professional secrecy (also known as legal professional privilege) which also applies to online communications.[19]

The core principle (b) of the CCBE Charter of the European Legal Profession concerns '*the right and duty of the lawyer to keep clients' matters confidential and to respect professional secrecy (and the resulting need to make reasonable efforts to prevent the unauthorised or unlawful access to confidential information)*.'

The CCBE Model Code of Conduct's Article on Confidentiality point 1 reads that: '*The lawyer is bound by confidentiality. It is a duty of the lawyer, and may also be a right of the lawyer.*' Point 4 of the same Article reads that: '*Confidentiality applies to any and all information about a client or a client matter which is given to the lawyer by his or her client or which is received by the lawyer in the course of the lawyer´s exercise of his or her profession, irrespective of the source of such information*.' Point 5 reads that: '*Confidentiality also applies to any and all documents prepared by the lawyer, to all those delivered by the lawyer to his or her client and to all communications between them*.' '*A lawyer shall respect the confidentiality of all information that becomes known to the lawyer in the course of his or her professional activity*.'

Professional competence

Lawyers are required to update and maintain their knowledge and professional skills. The core principle (g) concerns *'the lawyer's professional competence (and the resulting need to stay updated on the latest technological developments and their impact on the practice of law and lawyer's professional duties)*.'

[19] For more information on confidentiality of lawyer-client communications, see: 'Confidentiality of lawyer-client communications: a must for protecting your rights (2023)'

Model Article on Relations with Clients, point 2.2 reads that: '*Lawyers shall maintain their professional skills through continuing education in legal and other practice-related subject matters*.' The same point continues to clarify that: '*Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation. Lawyers are only able to provide such competent representation by keeping pace with the continuous rapid change of the law and technological environment in which they operate*.'

The duty of competence of the lawyer is thus not only restricted to law and regulation, but encompasses the obligation to become knowledgeable about a technical product to be used for professional activities. In the present context, such knowledge can effectively help the lawyer to assess and mitigate the risks related to the use of cloud services.

2. Understanding the risks associated with the use of cloud computing

It is important for lawyers to analyse and assess the risks of specific products and services that they intend to use. Based on the results of this assessment, lawyers should implement necessary measures to mitigate these risks and seek further advice where necessary. The aim to assess and manage risks in using cloud computing services is true for law firms of all sizes, small and large. Nevertheless, the sources of risks to be evaluated, the details of such evaluation and the possible measures for mitigating the risks depend on both the type and size of law firm, and the field the law firm works in.

Lawyers should keep themselves informed, for example, by following relevant training, to keep their knowledge on the applicable laws and regulations on cloud computing, cybersecurity, as well as professional obligations in these areas up to date. Bars and Law Societies should provide opportunities for lawyers to receive relevant information and training in these areas.

3. Ensuring compliance with deontological rules and data protection laws

Lawyers should make reasonable efforts to review and understand both relevant laws and national professional obligations in relation to the use of client data, first and foremost to prevent unauthorised or unlawful access to confidential information and information subject to professional secrecy / legal professional privilege. Particularly, lawyers should verify whether they are allowed according to the applicable deontological rules to store data outside their law firm and, if so, ensure that the cloud computing service provider is not subject to a jurisdiction with long-arm legislation obliging them to hand over European lawyers' data stored on a cloud server to, as the case might be, non-EU national authorities.

This involves a comprehensive understanding and adherence to the General Data Protection Regulation (GDPR), particularly focusing on the rules applicable to controllers, processors, data security and data subject's rights, as well as the rules for cross-border data transfers and storage.

This includes the obligation to notify the client of any data breaches, when appropriate and in consultation with their Data Protection Officer or the national Data Protection authority, as well as the steps taken to mitigate damages and prevent future incidents

4. Following available guidance

Lawyers should follow the guidance provided by regulators and Bars and Law Societies. The CCBE has also published a number of guidelines during the last decade which can also be helpful to lawyers using cloud computing services. These include:

- Recommendations on the protection of client confidentiality within the context of surveillance activities (2016)
- CCBE Guidance on improving the IT security of lawyers against unlawful surveillance (2016)
- CCBE Guide on Lawyers' use of online legal platforms (2018)
- Guide on the use of Artificial Intelligence-based tools by lawyers and law firms in the EU (2022)
- CCBE Guidance on the use of remote working tools by lawyers and remote court proceedings (2020)
- Annex to the CCBE Guidance on the use of remote working tools by lawyers and remote court proceedings: Analyses of videoconferencing tools (2020)

The CCBE published two sets of guidelines on GDPR:

- Recommendations regarding the implementation of the General Data Protection Regulation (GDPR) which provide assistance to Bars and Law Societies in preparing for the impact of national differences affecting how lawyers should work during the implementation efforts of the Regulation.
- Guidance on the main new compliance measures for lawyers regarding the General Data Protection Regulation (GDPR) which provide an overview of the main new compliance measures that Bars and Law Societies may wish to recommend in order to ensure compliance with the requirements set out in the GDPR.

5. Ensuring appropriate information security

Lawyers, regardless of the nature of their work or the size of their practice, must have in place the security measures to protect their IT systems, including the security of communicating with the client and storing clients' data.

Lawyers working with a large number of private and small business clients would be expected to use tools that are compatible with the solutions used by their clients. Such firms have to pay attention to the hidden costs of interoperability and cybersecurity, such as the loss of flexibility in terms of what IT products they can use due to security concerns, the difficulties in using IT assets the clients are providing, the costs of extra configuration and ongoing staff training, regular feature updates in cloud services breaking compatibility, etc.

Lawyers should consider requesting compliance of their suppliers with the applicable IT security standards, for example those developed by the International Standards Organisation (ISO) or the System and Organization Controls (SOC) developed by the American Institute of Certified Public Accountants:

- SO/IEC 27001:2022 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- ISO/IEC 27017:2015 – Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2019 – Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors[20]
- ISO/IEC 27036-4:2016 – Information technology — Security techniques — Information security for supplier relationships, Part 4: Guidelines for security of cloud services
- SOC 2 - SOC for Service Organisations: Trust Services Criteria Information security is not limited to technical measures only and should also include relevant policies and organisational practices to ensure the security of information and data processed by the practice.

Additionally, lawyers must be mindful to periodically review certification status (for ISO) or request new attestations (for SOC2) and understand what documentation is useful for their risk assessment.

6. Knowing the cloud services provider and the products / services they offer

Before using a storage and other cloud-based services, lawyers should conduct a risk assessment and carefully select their service provider. In particular, lawyers should carry out a qualified due diligence check on the legal guarantees offered by the provider they intend to engage for the provision of cloud services covered by professional secrecy/confidentiality. There are several broad types of information that should be taken into account in this exercise and these are listed below. This information may be included in the contract, terms and conditions of the service, privacy notices, cookie notices, or in technical descriptions, such as in Application Programming Interface (API) or other documentation aimed at developers and other technical specialists. Lawyers should use reliable sources of information in selecting the products or service, including verified websites, community websites or discussion forums, and feedback from other practitioners.

Lawyers should analyse the service level agreements in terms of their performance, security, data treatment and privacy and be aware that there are three different types of contract: mere adherence, negotiated, and mixed.

When doing so, lawyers should pay particular attention to the following aspects of a service:

- **availability and quality of support (customer service)** - the wider the scope of the services provided by a provider are, the more likely a lawyer user will have to rely on the customer services of that provider. In such a case, having a responsive and useful customer service of an IT provider is one of the most important aspects.
- **provider's financial stability and service history** – check the published financial reports and company registry details of the company, how long the same ownership structure existed and for how long did the given provider provide the same services to be acquired (e.g. by way of internet archive services).

[20] At the time of writing between June and October 2024 the revision of the standard was in progress.

- **availability and quality of information on the services provided** – the providers chosen should have good quality information on their services, including technical details (such as cloud infrastructure or platform providers, abbreviated as IaaS and PaaS).
- **transparency with regard to the subcontractors used** – the most useful information tends to be included in the privacy terms under sub-processors. The physical location of data storage tends also to be included in the privacy terms only.
- **compliance with relevant certifications, reports, and codes of conduct by the provider** – these are useful for lawyers to check since it may be difficult for them to otherwise assess the reliability of the technical capabilities of a service provider. Some of the codes of conduct include the CSA Star Registry[21], EU Cloud Code of Conduct[22] and SWIPO Code of Conduct.[23]
- **identity of the subcontractors** – when it is not possible for lawyers to verify the compliance using these codes or certifications, lawyers should aim to identify:
    - the subcontractors their chosen cloud provider will be using; and
    - the scope of the services of such subcontractors.
    - Some of the subcontractors may be covered by a relevant certification or code, which may give the lawyer some assurance as well. Importantly, however, the compliance of a subcontractor in relation to some parts of the total service may not always be relevant to the lawyer.[24]

      An alternative, more resource intensive approach, is for the lawyers to manually check what kind of provisions from the given code of conduct are present in the published terms and conditions of the cloud service provider. Even a partial compliance based on the public terms and conditions gives a more relevant picture of the service provider than not doing this exercise at all. If the published terms and conditions do not cover such information, lawyers should first try to acquire information directly from the provider or its reseller regarding these questions, and strive to include any assurances in the contractual terms entered into.
- **contractual terms** – where no technical solutions, certifications or codes of conduct help, lawyers should also check the contractual terms of the IT services for the following information:
    - periodical backups with high levels of physical and logical security;
    - mechanisms of authentication for the access to the information for lawyers of the law firm and clients;
    - encryption of the stored data;
    - registry of the accesses to the data;
    - security audit by a diligent third party;
    - use of user data by the provider: user data uploaded or generated in a cloud service used as a lawyer is not subject to any notion of "ownership" in the EU, and thus IT providers as data processors or data holders should not be able to claim any rights in relation to such data or use such data for any purposes other than what is simply necessary for the provision of the service to the lawyer. However,

[21] CSA Star Registry: https://cloudsecurityalliance.org/star/registry
[22] EU Cloud Code of Conduct: https://eucoc.cloud/en/home
[23] Code of Conduct for Data Portability and Cloud Service Switching for Infrastructure as a Service (IaaS) Cloud services Version: 2020, Date: 08-07-2020, available at: https://swipo.eu/wp-content/uploads/2020/07/SWIPO-IaaS-Code-of-Conduct.pdf
[24] This can happen when for example when the lawyer's IT provider will be able to move the data from its subcontractor supplier to another one – and that does not mean that the lawyer will be able to transfer his or her data to another provider.

considering the value of these large datasets and the difficulty of noticing such processing, such risk remains real. Such a use may be sometimes based on anonymised data, anonymisation is rarely a permanent and safe solution, thus it may entail considerable risks if done on the lawyers' data. For this reason, lawyers should seek clear assurances by the service providers in their terms that they will not use any customer data for purposes other than the provision of the service (regardless of these data being personal or non-personal).

- Jurisdiction and dispute resolution: While trivial for lawyers, it is still worth noting that even for lawyers, it may be very difficult in practice to enforce any rights set out in the terms and conditions if the courts having jurisdiction over the service contract are costly to reach for the given lawyer. Also, many SaaS contracts provide for mandatory arbitration or online dispute resolution, which is rarely beneficial from the viewpoint of small law firms seeking redress.
- Limitation of liability: Another, rather trivial point based on which lawyers may easily compare different service providers is the limitation of liability, or more probably, the upper amount of direct damages that the service provider undertakes to pay in the case of breach of contract. Just like most IT products, providers of cloud services also usually try to limit their own liability by excluding certain claims or categories of damages.
- Any penalties or service credits in the case of non-compliance with service level objectives: When comparing similar services and providers, those should be given preference that agree to provide at least a symbolic amount of penalty or service credit if they do not fulfil the service level objectives (such as downtime, response time etc.) promised.
- Term and termination of the services: lastly, prior to choosing a service, a lawyer should also understand how the service used may be terminated both at its own or the provider's initiative. The conditions should include a procedure for recovery and migration of data for the event of a contractual termination. Also, the lawyer should prepare the law firm's business continuity plan in line with the termination notice periods of the provider as stated in the contract. This also applies to data portability where lawyers should be able to retrieve data in a readable format for further use or for compliance purposes (e.g. tax).

7. Knowing where the data is processed

Lawyers must know where and how client data is processed. This includes verifying the legal and ethical permissibility of storing data outside of their firm, and understanding the differences in jurisdictions' data protection laws and whether data transfers outside of the EU are permitted, and if so, on what conditions. Lawyers should therefore be aware of the data transfer mechanisms used by their cloud service providers and the geographical locations they use for physically storing the data.

Transfer mechanisms

Under the GDPR, there are several transfer mechanisms that are set out in Chapter V:

- transfers with the adequacy decision[25]
- transfers without an adequacy decision.

If there is no adequacy decision, other appropriate data transfer mechanisms should be used. These include binding corporate rules, standard contractual clauses, codes of conduct and certification schemes, derogations under Article 49.[26]

- Standard Contractual Clauses are a model data transfer mechanism primarily designed to help controllers and processors legally facilitate data transfers to third countries.
- BCRs are legally binding and enforceable internal rules and policies for data transfers within multinational group companies
- Codes of conduct are a transfer tool developed by associations representing categories of organisations in a given sector.
- Certification is a new tool for data transfers to organisations which have been certified by certification bodies or data protection authorities in the EU/European Economic Area (EEA). This tool is still under development.
- Derogations under Article 49 GDPR allow for data transfers for specific situations, such as performance of a contract or defence of legal claims.

Following the judgment in Schrems II, the Court of Justice of the EU emphasised that organisations might need to implement extra measures alongside the appropriate safeguards when transferring personal data outside the EEA. The CJEU indicated that data controllers or processors, when acting as exporters, must individually assess whether the laws or practices of the non-EEA country, such as those mandating data access, undermine the effectiveness of the safeguards outlined in Article 46 of the GDPR.

Given the considerations earlier in this guide, lawyers should therefore be aware what regulations apply to the data stored by their practice and what measures they should take to protect the material falling under legal professional privilege, professional secrecy and relevant data protection obligations.

Lastly, since it is a fast evolving area and applicable data transfer mechanisms have been challenged in the past, lawyers should regularly monitor the relevant updates on legislation, case law and other information to stay updated on their obligations. This includes, among other things, geopolitical discussions on data security and potential state interference, such as backdoors or data flows to states, even when companies claim to process their data within the EU.

8. Knowing how data is processed

Given the omnipresence of cloud-based services, lawyers should be aware that even the simplest apps and solutions can include third-party data processing and further use. These can include text editing assistants, translation, image editing, etc. While this guidance does not intend to

[25] The list of countries covered by adequacy decisions is available here: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[26] EDPB guide on International data transfers

elaborate on these services, lawyers should nevertheless be aware of such processing possibilities and the related consequences.

9. Considerations on professional practice continuity

When lawyers store data remotely, they should ensure that the data can be retrieved and that the lawyer remains in control of the data. To this end, lawyers should have appropriate contingency mechanisms in place which include defining the categories of data, ensuring up to date local access to critical data and having an alternative internet connection.

Define and categorise critical data

Data should be categorised in terms of importance, and the so-called Recovery Point Objective (RPO): the maximum amount of time that can elapse between data backups before a loss of data becomes unacceptable from a business perspective. This is a decision to be consciously made by the lawyer. For critical services, it is in the lawyer's best interest to understand whether any local backups can be made of data from cloud services and if yes, how to carry out such local backups automatically.

Defining critical data is something that lawyers themselves have to define and understand. It should cover data that is (i) subject to obligations of retention by the lawyer, and (ii) without which a lawyer may no longer be able to provide effective assistance to a client. Such a definition should take into consideration the particular service rendered to the client, any contractual promises made to the client regarding the retention of the data in the engagement agreement, and the risks to the client in the absence of such a continuous legal service. Definition of critical data should also consider that some data may be recreated from third party sources (including from the court files or requesting the clients again to resend data that was lost).

Ensure up-to-date local access to critical data

The most important issue for a lawyer is to understand how to retain an up-to-date local copy of the most recent client data it has. This could include operating e-mail in a way that ensures that local copies (caches) of your mailboxes are always available (such as using IMAP, POP, .OST or third-party offerings for the largest e-mail service providers). Given the remarks on confidentiality above, lawyers should also consider whether these third-party providers have access to data that they process.

The same mechanism is needed for other, non-messaging related data stores as well, such as desktop clients or on-premise servers automatically synchronising with the cloud-based storage. Just having a technical possibility to download all such data is not sufficient, lawyers have to ensure that they can have such a copy of the critical data in consideration of the recovery point objective acceptable for the firm. There is also a risk that deleting copies on one device may result in their deletion from other devices linked to the same synchronised (shared) folder system. This risk is higher when multiple users share access to the same shared folder.

This is more of a problem if online practice or case management solutions store such critical data. Compared to the traditional cloud-based storage solutions, these tools are sold for fragmented

markets with relatively few customers, and even the most popular ones may not support automated local backups out of the box, and third-party solutions will also be lacking. This is an additional risk that lawyers should also take into consideration.

It is not expected from a practice management solution that all the data stored in that practice management system has to be available locally, but at least the critical data should be available in a way that local IT experts can technically recreate or make such data available for lawyers for further use, in the unlikely event of the sudden and permanent inaccessibility of the service provider. Simple promises in contractual terms and conditions cannot substitute the technical accessibility of critical data.

Have alternative internet access

No matter how much the use of cloud computing has increased, the weakest link from the viewpoint of the end user is still the accessibility of internet from the premises of the law firm. Thanks to advancement in electronic communications, alternative ways of accessing the internet could be available, such as having an alternative broadband provider in place (using a different distribution and core network than the original, not just a reseller of the same lines), or one or more mobile network accesses in place to which the law firm (or automatically any devices the law firm is using) can switch to when a backup connection is needed. Lawyers should ensure that they have such alternative arrangement when needed, and test such changeovers at least once a year. Moreover, for some law firms it might be advisable to think about a plan in case of a more generalised electricity or internet blackout. They should also consider saving critical data on a physical medium which is disconnected from the internet.

10. Having appropriate insurance cover

As lawyers hold sensitive and confidential client data, they should consider acquiring a cyber insurance coverage to protect against unwanted data breach costs, the costs of restoration of the business and of losses to the business activities as a result of a cyber-incident. Additionally, lawyers should review whether or not they are covered for damage claims by third parties resulting from cyber incidents such as ransomware attacks and also for damages resulting from hardware issues (which are often excluded from standard coverage).

Lawyers should also consider to negotiate a contract clause requiring the cloud service provider to maintain adequate insurance to cover their liability under the cloud agreement.

III. Conclusion

Cloud computing involves many risks and issues as outlined in these guidelines, particularly with regard to confidentiality/legal professional privilege and data retention. The CCBE invites Bars and Law Societies to increase awareness among their members for greater vigilance and to adopt high-level precautions. Legal and technical safeguards should be provided to them by their cloud computing providers (i.e. long-term data backup guarantee, etc.).

Bars and Law Societies are therefore encouraged to support lawyers' on questions regarding the use of cloud. Some Bars and Law Societies might even consider to develop private cloud computing infrastructures and services to both their individual and collective members in compliance with the above mentioned considerations. In this case, they may wish to carry out an impact assessment.[27]

[27] The CCBE is also examining how climate change on lawyers and their practice. To this end, it is developing guidance to help Bars and Law Societies consider the potential impact of climate change on the legal practice, which may be relevant to the use of cloud computing.