EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS
60 YEARS 1960 - 2020

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 Guidance on the use of remote working tools by lawyers and remote court proceedings

27/11/2020

The Council of Bars and Law Societies of Europe (CCBE) represents the bars and law societies of 32 member countries and 13 further associate and observer countries, and through them more than 1 million European lawyers.

In this paper the CCBE wishes to provide lawyers with some guidance on the use of remote working tools and on the conducting of remote court proceedings.

I. Introduction

It is often said that disruptive events may sometimes lead to radical new departures from the way things have been done in the past, but more often may simply accelerate trends which have been developing slowly for years.

This has been particularly evident in relation to the effect that COVID-19 has had on the ways in which lawyers perform their functions and interact with courts. For example, there has, for a number of years in a number of jurisdictions, been an increased acceptance of court hearings where at least one of the participants (for example, accused persons at procedural hearings or certain witnesses at trials) has been attending remotely. However, until the challenges arising from the COVID-19 pandemic, only the most tentative steps had been taken towards the holding of hearings which are entirely accessed remotely. With the restrictions on movement imposed by the relevant regulations in most European countries, these previously slow and tentative steps have been accelerated.

In many respects, legal systems have been in uncharted waters, and have been using new and unfamiliar tools. No doubt, many individual lawyers were already familiar with older business tools such as telephone conferencing, as well as having at least a nodding acquaintanceship with social media applications such as Facebook Messenger and Skype, but telephone conferencing has obvious limitations and what may be suitable for exchanging social pleasantries and pictures of cute kittens is not necessarily suitable for the administration of justice and for the conduct of confidential discussions which are protected by professional secrecy or legal professional privilege.

There are two inter-related aspects to the use of remote conferencing tools:

- Consultations and meetings by lawyers with their clients and others by remote means
- Remote participation in Court hearings.

There is a degree of commonality in the issues concerning each aspect; but each also raises particular issues.

II. The use of remote working tools by lawyers

There is a clear need for remote meetings, whether with clients, interviewing potential witnesses, internal management meetings, negotiations with other parties: whatever was normally done face to

face in a lawyer's practice needs to move online. At the beginning of the pandemic, there was already a number of tools available, but the challenge for the providers was to cope with the scaling up of their use, and for the user was to take tools which had been developed for one environment and develop them for another, more challenging environment, such as that of legal practice with its absolute requirement for confidentiality.

In that context, the following aspects stand out:

(a) *Fundamental Rights:* Issues related to fundamental rights will clearly arise in all cases where there is Professional Secrecy / Legal Professional Privilege but may do so in slightly different ways. All communications will be protected under Article 8 ECHR, whether in connection with prospective or pending litigation, or in connection with commercial negotiations, employment law advice, property transactions or any other of a myriad of other areas of a non-contentious nature where legal advice may be involved; whereas there will also be protected under Article 6 ECHR communications relating to criminal proceedings or commercial and other litigation. It will be recollected that Article 8 ECHR rights are qualified (albeit that lawyer-client communications enjoy a higher level of protection); whereas Article 6 ECHR rights are absolute.

(b) *Professional Secrecy / Legal Professional Privilege:* This will plainly apply whether the client is a natural or a legal person.

(c) *GDPR compliance*: This affects data subjects who are natural persons, so will plainly be engaged in dealing with clients who are natural persons. The engagement of GDPR where the client is a legal person may not appear to be so obvious, but in practice, there is likely to be the need to process personal data concerning natural persons whether they be employees, customers, persons with whom negotiations are being conducted etc., because behind every legal entity are natural persons.

These are areas of concern which require to be carefully considered when examining the terms and conditions of the various platform providers. Such an analysis is often far from straightforward, not least because the applicable terms and conditions may not necessarily be gathered together in a coherent whole on a single section of the relevant website. Often what a user needs to know to ensure compliance with GDPR and deontological obligations can be distributed across a number of documents – Terms and Conditions, Privacy Policies, annexes etc. each of which may be on entirely different sections of a website and not necessarily hyperlinked or cross-indexed.

In order to try to gain an understanding of the practical issues which arise in relation to legal practice, the CCBE prepared a number of individual research papers examining the terms and conditions of a number of frequently used platforms, in order to compare them[1]. As a result of this exercise, certain common issues emerged, namely:

1. How accessible and transparent are the relevant terms and conditions?
2. Who is the data controller?
3. Where are the data stored?
4. To what extent do the platform providers sell or share personal data?
5. To what surveillance might data held by Cloud platform providers potentially be exposed?
6. How technically secure is the platform?

[1] These papers may be found at [https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20201127_Annex_Analyses-of-videoconferencing-tools.pdf] and may form a starting point for further analysis. However, because the field moves so quickly, it is worth stressing that the papers may not reflect the changes introduced by providers after the research was conducted. The same is applicable regarding references to specific providers in the text.

1. Accessibility and transparency

Comment has been made above on the difficulty which is frequently encountered in trying to ascertain the terms and conditions and privacy policies which are applicable at any given time. This is compounded by the circumstance that the platform providers frequently change the terms and privacy policies, sometimes by bringing out new editions, sometimes by making unheralded alterations to existing terms which are often not even highlighted, so the only way to detect a change is by careful comparison between the older and the newer text.

It does not necessarily follow that difficulty of access equiparates to a desire to hide unfortunate terms – for example, the manner in which all of the relevant Cisco Webex terms is set out is of such Byzantine complexity that even the European Centre for Digital Rights, in its Report on Privacy Policies of Video Conferencing Services[2] analysed the Cisco terms as not being fully GDPR compliant, although the CCBE research subsequently revealed that the authors of the Report had failed to find a number of relevant contractual documents which were located (without a hyperlink) on another section of the website. Looking at the whole contractual terms, Cisco Webex had greater GDPR compliance than the Report had stated.

This lack of transparency of the terms and conditions has been commented upon by the European Data Protection Supervisor[3].

Throughout the individual CCBE research papers it was noted that the lack of clarity is not necessarily intentional and that, sometimes, it is disadvantageous not only for the customer but also for the platform provider. Be that as it may, the truth is that the terms and conditions of the platforms frequently contain complex provisions and exceptions. Furthermore, many of them must be complemented by other documents (normally also available in the webpage) such as privacy declarations and supplements or default data processing agreements.

2. Who is the data controller?

Platform providers have been on something of a learning curve as they enjoy greater take-up of their platforms by increasing numbers of users in increasingly diverse sectors. Some providers, notably some of those based in the United States, have woken up to the realisation that there are GDPR obligations which they have to meet and a new juristic vocabulary which they have to master.

Because of this, sometimes they state something which is plainly not so, for example, until recently, Zoom asserted that it could never be a data controller in respect of personal data which it was processing, and Microsoft, though taking a more nuanced approach, remains open to criticism as not having fully analysed situations in which it could actually be a data controller. In particular, the EDPS Investigation into EU Institutions' use of Microsoft Products and Services, referred to above, highlighted that Microsoft (and other providers) can act as a data controller in ways which are not always transparent, such as: the rights of service providers to amend data protection terms unilaterally; the limited scope of the data protection obligations in the Terms and Conditions, and the lack of specifically defined purposes for the processing which occurs under it.

While some platforms consider themselves data controllers (e.g. Kinly and Messenger Video), the terms and conditions of other platforms define the customer as the data controller, the platform merely being the processor. Even in the latter case, as has been observed, the provisions of the terms and conditions, taken as a whole may operate in such a way and grant powers and faculties to the

[2] https://noyb.eu/sites/default/files/2020-04/noyb_-_report_on_privacy_policies_of_video_conferencing_tools_2020-04-02_0.pdf

[3] This was also considered by the European Data Supervisor (EDPS) in its Public Paper on Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services (2 July 2020), see part 6

platform provider which are so wide that, in reality they also act as data controllers, despite statements in the Terms and Conditions to the contrary.[4]. This is the case, for example, of Zoom (until a recent change in its standard terms), Microsoft Teams and Cisco.

3. Where is the data stored?

The terms and conditions of many platforms contain no guarantee that data is stored in any particular country, nor even within the EU. This plainly raises an issue in respect of GDPR compliance.

In the case of platforms such as Messenger Video, Skype, Skype for Business, BlueJeans and Cisco, it is clear that the data collected in the European Union may be transferred and stored outside the EU (mainly but not only in the US). In some other cases, it is not easy to identify the State in which the data will be stored because there are several data centres, as seems to be the case for Kinly and StarLeaf. Another example is Microsoft Teams, according to whose terms, depending on the country of location of the data controller (i.e. the customer) and on the type of data, the place of storage of the latter will vary. It is worth noting that, for data controllers in many EU countries, at least some of the data which they control will be stored outside the EU[5]. This might suggest that due diligence should include seeking, so far as possible, to use platforms whose servers are hosted in the EU; and that if that is not possible, seeking to conform to the recommendations and decisions of the European Commission, EDPB and the relevant national Data Protection Authorities in relation to international data transfers.

The problem is compounded by the circumstance that many of the US-based providers relied upon self-certification under the EU-US Privacy Shield to regularise such data transfers, but the decision of the CJEU in the *Schrems II*[6] case setting aside the Privacy Shield has prevented the use of this mechanism. Although, the judgment does uphold the continuing validity of Standard Contractual Clauses, there is still a need for constant vigilance. The CJEU pointed out that the need for additional safeguards must be verified on a case-by-case basis, which is why the debate on the effectiveness of such clauses continues.

4. To what extent do the platform providers sell or share personal data?

Most platform providers' terms and conditions state that, in general, data will neither be sold nor shared except insofar as otherwise permitted by the terms and conditions themselves.

Sometimes, such statements should not be taken at face value, as definition sections within the terms and conditions may give specially defined meanings to words like "sell". For example, one provider's terms stated that transferring data to someone else for a money payment does not count as "selling" if the transferee has similar terms & conditions to the provider.

Further, within the terms and conditions, there are usually exceptions under which providers can, indeed, share customer data with certain third parties under certain conditions. The implications of these exceptions are frequently not clear. For example, most of the platform providers are permitted to share data if necessary with third parties such as business partners, auditors, legal advisors, subsidiaries and corporate affiliates. In addition, they may also share data for some other reasons, including to comply with legal obligations or as part of corporate transactions such as mergers or sales of assets. In some cases, the lack of transparency of the terms and conditions and predictability of their

[4] This was also considered by the European Data Supervisor (EDPS) in its Public Paper on Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services (2 July 2020), see part 2

[5] This was also considered by the European Data Supervisor (EDPS) in its Public Paper on Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services (2 July 2020), see part 4

[6] *Judgment of 16 July 2020, case Schrems II*

effect is particularly problematic, with wide and vague exceptions permitting the sharing of data for reasons such as enforcing the provider's policy and agreements, implementing the provider's business operations or protecting the right of property of the platform provider.

5. To what surveillance might data held by Cloud platform providers potentially be exposed?

A particular concern under this head is the danger arising from so many of the leading platform providers being based in, or having places of business in the United States, where they are subject to the long-arm jurisdiction of the Cloud Act. The Cloud Act enables US courts and authorities to request personal data from US companies storing it on cloud servers within the European Union. The question of the justification of data transfers in the context of the Cloud Act has been addressed by the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) in a joint response to the LIBE Committee. In this response, they take the view that, in the event of a request based on the Cloud Act without an international agreement corresponding to Art. 48 GDPR, a transfer of data can only be justified if necessary to protect the vital interests of the data subjects[7].

6. How technically secure is the platform?

The technical safety of platforms seems not to be a major problem, but there are, nonetheless some vulnerabilities.

Some of these vulnerabilities relate to the defaults on the user settings and can easily be addressed if the user is alive to the risk and takes steps to change the user settings. For example, it was notorious that, at the outset of lockdown, the default user settings on Zoom were set to minimum security levels, allowing very easy access to unauthorised participants, and giving a new word to the English Language: Zoom-bombing. The settings were capable of being set by the user to give greater security levels, but it is remarkable how many users did not implement the necessary steps. However, being sensitive to market pressures, Zoom responded by changing its default settings to provide higher levels of security, and this particular problem has now largely disappeared.

However, there are other security vulnerabilities which are inherent in the platforms and not so easily addressed. This is particularly so in relation to the nature and extent of the encryption provided.

Some, but not all platforms offer end-to-end encryption. Microsoft, for instance, does offer end-to-end encryption, whilst other platforms, such as Cisco, provide for standard encryption by default, offering end-to-end encryption only as an additional option. It has been reported that other platforms, such as Zoom, at the beginning of lockdown, provided “encryption” which was neither end-to-end nor in compliance with international standards on encryption, although that is something which Zoom has since addressed.

7. Are there impediments to the availability of remedies?

The Terms and Conditions usually contain choice of law and exclusive jurisdiction clauses. It is worth bearing in mind that these (particularly the latter) may present practical barriers to the obtaining of remedies. This is especially problematic as many providers have clauses conferring exclusive jurisdiction on a particular state or the federal jurisdiction in the United States (and, sometimes in a specified court in a specified city), though some, notably Cisco, provide for jurisdiction in at least one European jurisdiction.

[7] ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence: https://edpb.europa.eu/sites/edpb/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf

Conclusions regarding the use of remote working tools by lawyers

As the foregoing discussion discloses, there is a constant need for lawyers to read, understand, and periodically review the terms and conditions of platforms which they use so as to ensure that they properly observe their data protection and deontological obligations.

The various platforms provide different standards of reliability, robustness, user experience and the like, and there may be a natural tendency to choose the one which gives, subjectively, the best experience and the most useful features. That is largely a matter of taste, but, in the final analysis, choosing an appropriate tool depends not only on such factors but also on a careful consideration of the great unseens – GDPR compliance, protection of confidentiality, robustness of the terms and conditions from the point of view of the user. Further, as the above discussion discloses, this is a review exercise which cannot be carried out only once but needs to be performed constantly.

III. Remote Court Proceedings

Different courts in different jurisdictions conduct remote proceedings using different platforms. Although the same issues as discussed above are still there, they are likely in practice to be of lesser concern to lawyers as it is the Court which is likely to be the Data Controller, rather than the lawyers. In any event, court proceedings are usually held in public and, in some jurisdictions, once documents are referred to in court, they become public documents. Further, it may also be that in some jurisdictions, the act of disclosing them to the judge and the other side will mean that Professional Secrecy/ Legal Professional Privilege will no longer attach to them, whereas in other jurisdictions the act of disclosing documents to the judge and the other side has no impact on the lawyers' duty to observe Professional Secrecy regarding these documents.

However, this does not mean that Bars and Law Societies and individual lawyers can ignore the privacy and data protection issues. A real-world example can be given from England and Wales where, at an early stage of the pandemic, there was a proposal coming from the Court Service that proceedings before the Family Court in England and Wales would proceed by way of Zoom. This was especially concerning as the data arising from such proceedings will often be special categories of personal data, and such proceedings would normally be held in private. It was, therefore, necessary to point out to the court administration these particular concerns as well as the generic ones which had been expressed about the Zoom platform in the state in which it stood at that time.

More likely to be of concern on a day to day basis is the question of delivering an Art 6 ECHR compliant fair trial. Of particular note is the requirement for there to be parallel secure private channels accessible by the respective clients and their legal teams[8].

Anecdotal evidence suggests that most courts are not providing this facility, but that the relevant legal teams are making their own *ad hoc* arrangements (separate platforms; email; chat groups on various platforms etc.) There is a question as to whether this is legally adequate to ensure a fair trial, especially if there are different levels of technical expertise in opposing teams, and practical problems as to how best to use such parallel channels.

More significantly, once lawyers provide their own channels, that re-awakens the same issues which arise in relation to remote meetings as discussed above. For example, if a lawyer were to set up a parallel channel using, say, a group chat on Facebook Messenger, then the chat (which would very much be subject to PS/LPP) would be retained by Facebook on its servers and subject to surveillance under the Cloud Act. Perhaps the medium used might be What's App which is, certainly, technically more secure. However, the problem remains that the medium used for such a parallel channel may

[8] Sakhnovskiy v. Russia (Application no. 21272/03); and Marcello Viola v. Italy (Application no. 45106/04).

not be one which would be used by the lawyer for other remote business; which does not excuse the lawyer from having to perform, in relation to that channel, the same sort of due diligence which has to be employed in considering what remote conferencing facility to use.

There would be other issues not of a purely IT/Surveillance nature inherent in remote proceedings. For example, in relation to equality of arms: disadvantage to parties lacking access to IT, the effect of poor internet speeds, the difficulty for a judge to effectively to assess the credibility of a witness without seeing the witness in the flesh, the problems with security of remote connections (how is it knowable whether, metaphorically or literally, the man holding the camera in front of the witness is not also holding a gun?). Certainly these arguments cannot be entirely excluded in real proceedings: it can also be argued that parties lacking access to IT are also lacking the means to afford legal assistance and that a witness can be influenced in other ways before a court hearing, for example by threats. Nevertheless, they need to be considered.

These and other matters were discussed in a CCBE Paper on the Use of Videoconferencing in Criminal and Civil Cases which were based on the CCBE position on the proposals for amending the regulations on service of documents and the taking of evidence in civil and commercial matters (19/10/2018). The following generic remarks made in that paper, which are relevant for proceedings in both civil but even more in criminal and civil matters, are also worth highlighting here:

- Before reaching a final determination on which videoconferencing ("VC") program to use, courts and judicial authorities should implement their VC system using a pilot program that they can evaluate and modify. Courts should set up a system where, following a VC, they receive feedback from all participants on the VC's organization in order to further improve their VC system. Additionally, courts should provide structured training for judges and anyone who will operate the VC equipment during the hearing, as well as ensuring the proper training and availability of IT staff. They should also share VC best practices with each other in order to reduce costs and increase efficiency.

- Contingency plans need to be in place in order to deal effectively with issues such as dropping or bad connections during the VC session.

- In cross-border cases, particularly where the parties might not be native speakers and will be subject to different cultural influences, the judge might not be able to examine so easily the nuances of the parties' appearance and responses through a video-link. Moreover, judges might have a tendency to ask fewer questions and be less likely to interrupt an argument, which might not be a beneficial outcome for the parties.[9] Therefore, it is important that proper technical arrangements are made in order to ensure so far as possible a true-to-life hearing experience including full communication and interaction of all the parties to the procedure with the witness or other person who is being examined. Consumer-level videoconferencing services, such as Skype or FaceTime, are inadequate in this respect.

- In some jurisdictions, the use of VC might be subject to the parties' approval. Relevant questions are thus: Is it necessary to seek the consent of the parties to participate in a VC? Under what conditions can parties refuse a VC? Does legal counsel need to be present or consulted if parties consent or refuse?

- The extremely important issue of ensuring respect for professional secrecy/legal professional privilege when using different online tools for remote proceedings has already been discussed above. As also noted, during a VC session, the lawyer needs to be able to confer confidentially with his/her client (whether the lawyer and client are sitting together or are remotely situated from each other). Relevant questions are thus: is the confidentiality of lawyer-client

[9] *See e.g.* Report of a Survey of Videoconferencing in the Court of Appeals, M. Dunn and R. Norwick, Federal Judicial Center, 2006, available at: http://www.fjc.gov/public/pdf.nsf/lookup/vidconca.pdf/$file/vidconca.pdf.

communication guaranteed in all jurisdictions participating in the VC? If not, the parties' interests might be endangered. Can the VC be recorded? In case of a breach of confidentiality involving a VC, who bears professional responsibility for it? What technical requirements should be respected in order to ensure that the VC is protected from improper access (hacking)?

- The court/judicial authority needs to notify the parties, including their lawyers, of the data, time, place, and the conditions for participation in the VC. Sufficient advance notice should be given. In this context, how long should the notice be in order to be regarded as sufficient?
- Arrangements need to be made in order to enable the lawyer to participate in the VC. The lawyer should be able to sit together with his/ her client. If this is not possible, arrangements must be made in order to enable the lawyer to participate in the VC from another location.
- Where local rules require a participating lawyer to provide evidence of his identity and entitlement to appear, the lawyer needs to be enabled to do so, remotely where necessary.
- Instructions need to be provided to the lawyer by the relevant court/judicial authority as to the procedure which requires to be followed in order to present documents or other material during the VC. Arrangements need to be made to ensure that all participants in the VC can see any material that is presented during the VC.
- In cases where documents have to be shown to a witness, that should be done via an independent person present with them (court clerk or similar) who can ensure (e.g. from the point of view of the prosecution) that they are looking at the right page and (from the defence point of view) also ensure they are not looking at other documents, especially not at documents that have not been disclosed to the defence or other parties.

These concerns are relevant in respect of both criminal and civil proceedings. However, the answer to the question if, in a specific case, remote proceedings can be seen as an appropriate way to conduct proceedings may certainly differ depending on the nature of the case (i.e. whether it is a criminal[10] or a civil case; the gravity or importance of the case, the parties involved etc.).

Practical experience during the pandemic has shown that there are differing approaches both within and between jurisdictions. Where proceedings do not take place in the time-hallowed manner of all the participants being present in court at the same time (now usually with social-distancing measures being in place), proceedings often take place on remote conferencing platforms, or occasionally, by telephone conference call. Sometimes the proceedings are hybrid in nature, with some participants taking part in person and others remotely. An interesting example of the latter is the conduct of criminal trials in Scotland, where all of the participants are present in court in person, (though with social distancing) although with a possibility for a witness to participate by videoconference where, exceptionally, that is required. However, Scottish juries consist of fifteen people, and that presents obvious challenges to achieving social distancing. Accordingly, the jurors participate remotely from "remote jury centres" (in reality, auditoria in multiplex cinemas which have been rented by the Scottish Court Service) with the proceedings relayed to them, and the image of each individual juror transmitted back to a bank of screens in the court.

The current situation gives us also a chance to consider new approaches to traditional court proceedings in civil matters like the Canadian Civil Resolution Tribunal (CTR), which is worldwide one of the first examples of online dispute resolution (ODR) being incorporated into the public justice system[11].

---

[10] See, for example, the European Criminal Bar Association's (ECBA) Statement on videoconferencing in criminal cases (6 September 2020), where the question of in what type of criminal cases videoconferencing could be used, is discussed.

[11] https://civilresolutionbc.ca/

It is clear that there is no “one size fits all” solution; but what is also clear is that, whatever solution is adopted, the above principles will require to be followed in order to provide a fair trial.

IV. Conclusion

The COVID-19 pandemic has forced rapid changes in the way in which we all work, and lawyers are not exempt from these changes. The practice of law has always depended on the need to engage directly with others: lawyers with their clients, with their opponents, their negotiating counterparts, witnesses and the court, yet the way in which those encounters have taken place have, through necessity, changed. It has not always been a change for which lawyers, judges, and justice systems have been prepared, and there has inevitably been a feeling of the way, false starts, and sudden changes.

Lawyers and other users of remote systems are not alone in facing these challenges, and often the IT industry, and in particular, the providers of remote conferencing systems have needed to scale up their businesses and, in so doing, cope with both the technical and legal issues which arise from that growth.

The result has been a constantly moving, changing and unfamiliar landscape, with sudden new challenges coming out of nowhere, and the need to develop rapid and novel responses. This challenge must be seen as a great opportunity that can drive forward the digitization of our society and our judicial systems.

Yet, despite this constant state of flux, certain values remain unchangeable – the respect for professional secrecy and legal professional privilege, compliance with data protection and deontological obligations and the over-arching requirement to provide a fair trial.

In these circumstances, though lawyers and justice systems should not be afraid to meet the challenge of working in new ways, this is not something which can be done blindly, unheedful of the very real issues which require to be addressed. Lawyers require constantly to be addressing these issues, remembering that the landscape continues to change from day to day

It is with this very much in mind that this paper seeks to provide, if not a comprehensive guidebook to the new world of remote working, then at least a few signposts and some hopefully useful guidance to the perplexed.