**Video Conferencing Security**

The COVID-19 crisis is changing the way we live our lives. Keeping our distance means many of us are working from home for the first time and adapting to new ways of doing our jobs.

Thankfully, technology is helping us all stay connected. Video conferencing software and apps are valuable ways of doing business, holding staff meetings and keeping in touch with colleagues. Members have asked if this could include BCRP Exclusion meetings and yes it can, provided you have the right controls, training and policies in place.

With everyone working under such extraordinary circumstances, it’s easy to prioritise convenience over security. The ICO has offered advice to help – combining the efficiency of digital connection with the necessity for privacy protection.

Here, is advice you can share with your members to ensure they can communicate with confidence.

**Have you checked the privacy and security settings?**

Video conferencing technology must be transparent. Users need to know how their data will be processed, as well as having choice and control over it. So, you should make use of privacy and security features. These can include restricting access to meetings using passwords, controlling when people can join the meeting or controlling who is allowed to share their screens. Think about who and how you share the meeting ID or password.

Make sure confidential material is not visible in the background and consider using a backdrop screen.

You should make these choices before you start the meeting and consider providing members with clear advice on which features to use and how.

**Are you aware of phishing risks?**

Many of us are aware of the signs of phishing emails or texts, but would you know what to look out for in a video chat? The ‘live chat feature’ can be used by malicious people to spread phishing messages. Be vigilant. Do not click on links or attachments you were not expecting or from meeting attendees you do not recognise.

* **Meeting Bombing** – In this type of attack, an uninvited guest joins a video conferencing meeting either to listen in on the conversation or to disrupt the meeting by sharing inappropriate media. These incidents are possible when:
	+ You do not require a password.
	+ The attacker is able to discover or guess the meeting ID, known as war dialling. War dialling software makes it possible for the attacker to find out the meeting ID, as well as information about the meeting including the meeting name and the meeting organizer.
* **Malicious Links in Chat**– Once attackers gain access to your meeting room, they can trick participants into clicking on malicious links shared via the chat, allowing attackers to steal credentials. This reinforces that it’s more critical than ever to require passwords for all meetings.
* **Stolen Meeting Links**– Reusing meeting links makes it easy for attackers to use them too. To avoid unauthorized access to your meetings, turn on notifications that will let you know when someone has joined your meeting room without you. Or better yet, don’t allow others to join your meeting before you do by disabling “Join Before Host.”
* **Data Shared With Third Parties** –

Software as a service (**SaaS**) is a software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet. **SaaS** is one of three main categories of cloud computing, alongside infrastructure as a service (IaaS) and platform as a service (PaaS).

For SaaS services, first, ensure security controls are in place to protect your data, and then ensure those controls are configured properly. SaaS security solutions, like Prisma SaaS, automatically detect and remove the sharing of files that have confidential or personal information. For non-SaaS services, it’s important to have data protection agreements in place with third parties that address appropriate security controls; for example, data encryption, role-based controls for authorized users to access, etc.

**Malware or Zero Day Attacks**– When it comes to zero day attacks, legacy anti-virus software is no match. You will need to protect from malicious activity by layering security at the endpoint and in the network

(Some define zero-day attacks as attacks on vulnerabilities that have not been patched or made public, while others define them as attacks that take advantage of a security vulnerability on the same day that the vulnerability becomes publicly known).

**Have you checked your organisation’s policy?**

Whilst you may have a preferred app to keep in touch with your friends and family, you should check to see which tool your organisation has chosen to use. Organisations should select a video conferencing platform that matches their policies.

**Have you ensured all software is up to date?**

One of the most effective security measures you can take is to keep all your software up-to-date, and video conferencing software is no exception. If you have installed a video conferencing app, keep it up to date by applying all available software updates regularly. You may well have configured your equipment to do this automatically. If you access a video conferencing service via a web browser, then make sure the browser is kept up to date too.

**Is this still the right tool for the job?**

In a time of crisis, decisions are often made quickly to get the job done. But in the long run, circumstances can change, and the risk balance case might look different. There is no reason to remain committed to using a particular tool or service forever just because you used it in an emergency. Re-visit your decision when you eventually have time and resources to do so.

## **Selection of an appropriate video conferencing tool**

At the selection stage you should take a closer look at the data protection regulations to comply. You should pay attention to the following points:

### VIDEO CONFERENCING SOLUTION FOR BUSINESS

Business Versions are suitable for both internal company communication and conferences with customers and business partners. Only these versions usually offer the required security standards. Consumer-grade or unlicensed software are not suitable for business video conferencing.

### PREFER EU PROVIDERS

Video and online conferencing tools from providers located in the European Economic Area should be preferred, as they are directly subject to the provisions of GDPR.  If you plan to use the video conferencing system of a third country provider, it must be ensured an adequate level of protection data protection comparable to that in the EU.

### DATA PROTECTION OFFICER

The DPO should be involved in the selection of an appropriate video conferencing system. They ensure that the data protection rules are respected.

### DATA PROTECTION BY DESIGN

The GDPR requires you to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the GDPR’s fundamental principles and requirements. When choosing a video conferencing tool, you should in particular watch out for:

* + - Video transmissions should use end-to-end encryption.
		Caution applies here for persons subject to professional secrecy: a video conferencing tool using a system that transmits data over the network in unencrypted form constitutes a failure to comply with the obligation of secrecy.
		- Use password protected meetings to keep unwanted participants out.

## **Before first use: what you need to know**

Before using the selected video conferencing service for your meetings, you should also consider the following points:

### USER CONFIGURATIONS (VERY IMPORTANT).

To accomplish the required security level, it is necessary to adjust the settings manually. If you are planning to use tracking, observation, logging, screen-sharing, and recording functions, you should always ask whether it is necessary to use these functions.

Some systems by default, only allow the host to initiate a Local Recording. If another participant would like to record, the host will need to provide permission to that participant during the meeting. ... If a user has scheduling privilege for you, they will automatically join as an alternative host and be able to start the recording. **It is strongly recommended that you do not record conferences where personal data is shared.** Why would you need to do this and remember that the data will be stored on your own computer but may also be automatically stored in the cloud. **CHECK YOUR SETTINGS.**

### SCREEN SHARING

Only information, which is relevant for the meeting, should be displayed. Close all content that is not required. E.g., you could use a second desktop with no files or shortcuts on it.

### EMPLOYEE TRAINING

Before the first use all members should be informed which data is allowed to share via the video conferencing service. The exchange of documents should be avoided if it contains confidential information. Furthermore, it should be ensured that no personally identifiable information is exchanged via the chat function. As previously explained depending on the provider it cannot be excluded that recordings of the chat progress are saved after the end of the conversation.

### INFORMATION IN ACCORDANCE WITH ART. 13 GDPR

You must provide attendees with information about the processing of personal data in the context of video conferences. The relevant information can be included in the e-mail invitation. It is advisable to have a Confidentiality Agreement agreed before the start of every meeting.

<https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed-1-0.pdf>

**Risk management in the use of video conferencing**

Within the IT infrastructure, security teams are aware of the need to evaluate critically the used tools, services and resources in terms of their intended use. In addition to the widely described data protection aspects, cybersecurity ratings are playing an important role in corporate risk management. The evaluation of third parties or their tools and applications is particularly important when situations and scenarios change almost daily, and decisions have to be made under high pressure. Due to the current increase of employees working from home the threat level is rising. Studies show that home networks pose a significant cybersecurity risk (malware infections, phishing attacks, etc.).

Within the risk management of your partnership, a cybersecurity rating can be supplemented easily and practically. Such a rating takes a three-dimensional view of the environment of your company or a third party (e.g. a video conferencing tool that is planned to be introduced).

The main indicators, such as the use of certificates, patch and update levels, encryption technologies, spam distribution and the presence of compromised end devices and servers are checked. Therefore, the rating provides valuable information about the resistance of the own security eco-system to various attack scenarios.

In view of the expected increase of employees in home offices and the general rise in the use of video conferencing tools, it is advisable to have a stable cybersecurity management system as part of your risk management.

**Cybersecurity Audit Checklist**

* Management. Company **security** policies in place.
* Employees. Training on phishing, handling suspicious emails, social engineering hackers. ...
* Business practices. Emergency and **cybersecurity** response plans. ...
* IT staff. System hardening plans. ...
* Physical **security**. ...
* **Secure** data. ...
* Active monitoring and testing.

**(See Appendix A)**

## **GDPR and privacy implications of using such services?**

### ASK FOR A DATA PROCESSING AGREEMENT (DPA)

### Video conferencing services such as Zoom, GoToMeeting, etc. are no different than any other online service provider – if they’re processing any personal data from your use of the service, they will be your data processor and in GDPR terms that means you need to be sure they are GDPR compliant and that you apply the GDPR Article 28 requirements to ensure there is a contract in place with regard to the processing of that personal data. And, yes, that includes when you have a team meeting or invite people to an online discussion via the service (because of the wide definition of processing in GDPR).

There are a couple to things to consider:

* You, as the host (i.e. the organiser of the online conference) will be the data controller. This means that you will need to consider the implications of what you need to do when it comes to being a controller (right to be informed, what you’ll do with the data, the fact that any data you process via the system is covered by GDPR, etc.) as you will be processing personal data
* As the video conferencing provider is online/cloud-based they will be your data processor. The GDPR requires you to ensure any processors you use are GDPR compliant and that there is a controller-processor contract (sometimes called a data processing agreement or DPA) in place. You will also need to be clear and understand what the provider does with data that it may collect from your (and your attendees’) use of the system

As a controller:

* Decide how you plan on using any information, recordings, attendee lists, etc. you will be processing from the session and consider the GDPR implications and lawful basis for processing. You will need to provide (via your privacy policy) information about this to attendees (and sign-post that information appropriately). Don’t forget the right to be informed, individuals’ rights, etc. all apply to both any registration data you collect, information recorded during the session, how you’ll use the data, etc. To identify these considerations and risks from the processing, I would suggest you carry out a Data Protection Impact Assessment (DPIA) as this will also demonstrate you’ve considered carefully what data you will be processing and any inherent risks from that processing (and don’t forget about any features available to you that the attendee may not know you have access to, such as Zoom’s ability to tell you whether someone is paying attention or not)
* If you plan on recording the session, you should make it clear to the attendees that this will be happening and what you plan on doing with the recordings and/or transcripts (e.g. sharing with all attendees) and spell out the implications for the attendees (e.g. if they turn on their camera their image will be available to everyone in attendance, depending on how they set up their account, their name, email, etc. may be available to other attendees, what they say will be recorded, etc.).
* Also, be clear that if they screen share or discuss confidential (or special category) information, this too may be retained as part of the recording, so they should be mindful of their own privacy requirements – you may need to seek consent for such special category data processing or stop the recording!
* Carry out due diligence on the service provider to ensure you are happy they are GDPR compliant – you should already have a process for this as this is no different than any other online service that processes personal data for you (e.g. your CRM, email list provider, etc.). You should pay particular attention to what the service provider says they will do with recordings and data they collect on your behalf – you should find this in their privacy policy and/or in any GDPR statements they provide about how they are ensuring GDPR compliance. And remember that they may be processing this data outside the EU. In settings you can choose in which region your data is stored to ensure the security of this data and compliance with EU standards?
* Make sure you sign a data processing agreement (whether separate or part of terms of service) that meets the contractual requirements set out in Article 28

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/what-needs-to-be-included-in-the-contract/>

**Appendix A**

There are hundreds of items that could be on a cybersecurity audit checklist. Here are some broad categories and ideas that cover many of the crucial cybersecurity threats:

1. **Management**
	1. Company security policies in place
	2. Security policies written and enforced through training
	3. Computer software and hardware asset list
	4. Data classified by usage and sensitivity
	5. Established chain of data ownership
2. **Members**
	1. Training on phishing, handling suspicious emails, social engineering hackers
	2. Password training and enforcement
	3. Training on dealing with strangers in the workplace
	4. Training on carrying data on laptops and other devices and ensuring the security of this data
	5. All security awareness training passed and signed off ensuring that all members not only understand the importance of security but are active guardians for security
	6. Ensure that Secure Bring Your Own Device (BYOD) plans are in place
3. **Business practices**
	1. Emergency and cybersecurity response plans
	2. Determine all possible sources of business disruption cybersecurity risk
	3. Plans in place to lessen business disruptions and security breaches
	4. Emergency disaster recovery plans in place
	5. Alternative locations for running business in case of emergencies or disruptions
	6. Redundancy and restoration paths for all critical business operations
	7. Have you tested your restoration and redundancy plans?
4. **IT**
	1. System hardening plans

***Systems hardening*** *is a collection of tools, techniques, and best practices to reduce vulnerability in technology applications, systems, infrastructure, firmware, and other areas. The goal of systems hardening is to reduce security risk by eliminating potential attack vectors and condensing the system’s attack surface. By removing superfluous programmes, accounts functions, applications, ports, permissions, access, etc. attackers and malware have fewer opportunities to gain a foothold within your IT ecosystem.*

* 1. Automated system hardening on all operating systems on servers, routers, workstations, and gateways
	2. Software patch management automated
	3. Security mailing lists?
	4. Regular [security audits](https://reciprocitylabs.com/cloud-security-vs-traditional-security/) and penetration testing
	5. Anti-virus software installed on all devices with auto-updates
	6. Systematic review of log files and backup logs to make sure there are no errors
	7. Remote plans in place, as well as policies regarding remote access
1. **Physical security**
	1. Lock servers and network equipment
	2. Have a secure and remote backup solution
	3. Make sure keys for the network are in a secure location
	4. Keep computers visible
	5. Use locks on computer cases
	6. Perform regular inspections
	7. Prevent unauthorized users from entering the server room or even in the workstation areas
	8. Security camera monitoring system
	9. Keycard system required for secure areas
	10. Secure Data Policy in place and ensure users understand the policy through training
	11. Secure trash dumpsters and paper shredders to prevent dumpster diving
2. **Secure data**
	1. Encryption enabled wherever required
	2. Secure laptops, mobile devices, and storage devices
	3. Enable automatic wiping of lost or stolen devices
	4. Secure Sockets Layer (SSL) in place when using the Internet to ensure secure data transfers
	5. Secure email gateways ensuring data is emailed securely
3. **Active monitoring and testing**
	1. Regular monitoring of all aspects of security
	2. Regularly scheduled security testing
	3. External penetration testing to ensure your staff has not missed something
	4. Scanning for data types to make sure they are secure and safely stored

David Wilson

NABCP