GRA
GIBRALTAR REGULATORY AUTHORITY

(22) Video Conferencing

Guidance on the EU General Data Protection Regulation 2016/679 & Data Protection Act 2004

21st October 2020

Guidance Note IR04/20

FOREWORD

The EU General Data Protection Regulation 2016/679 (the "GDPR") came into force on 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive 95/46/EC.

Her Majesty's Government of Gibraltar amended the Data Protection Act 2004 (the "DPA") on 25th May 2018, in accordance with the introduction of the GDPR. The DPA complements the GDPR and also implements the Law Enforcement Directive 2016/680. Therefore, the DPA and the GDPR must be read side by side.

It is important to note that the GDPR does not generally require transposition (EU regulations have 'direct effect') and automatically became law in Gibraltar. Therefore, organisations involved in the processing of personal data need to be aware of the obligations that the GDPR and/or the DPA will impose on them. The GDPR emphasises transparency, security, and accountability by data controllers, while at the same time standardising and strengthening the right of European citizens to data privacy.

The Gibraltar Regulatory Authority, as the Information Commissioner, is aware of the increased risks to privacy posed by the use of Video Conferencing Applications ("VCAs").

The Information Commissioner's aim is therefore to alleviate some of the concerns for organisations and individuals alike, and increase their awareness to ensure data protection compliance, in particular, when using VCAs.

SUMMARY

- The COVID-19 pandemic has resulted in a sharp uptake in the use of Video Conferencing Applications ("VCAs"), increasing the risks surrounding collection and use of personal data.
- This document provides guidance to individuals on how to protect their personal data and privacy when using VCAs; as well as guidance for organisations on data protection compliance when using VCAs.
- The following summarises the guidance provided by the Information Commissioner below:

INDIVIDUALS

- **Research** the different services available.
- Familiarise yourself with the **security and/or privacy settings** available, and ensure **passwords** are strong and unique.
- Ensure that sessions are **only accessible** to the targeted participants and refrain from **unnecessarily disclosing personal information** during calls.
- Be wary of **your surroundings** as this may be captured by your webcam.
- Consider the need to **update software** to protect against vulnerabilities.
- Consider the **data protection and privacy rights of other participants** before you post or share information.
- If you are using **a web browser**, open the video conferencing session on a new window to avoid inadvertently sharing information. Also consider turning off **smart speakers**.
- Be wary that video cameras and microphones might be **on by default** when joining a call.
- Check whether the video conference is **being recorded.**
- Do not open unexpected video conference **invitations or links**.

ORGANISATIONS

- Consider the implications of VCAs and their compliance with data protection laws, to choose the one **best suited to your organisation's needs**.
- Establish appropriate **technical and organisational security measures** to protect personal data when using VCAs.
- Establish **data protection policies** where proportionate.
- Consider **transparency and fairness** when using VCAs, particularly if monitoring staff.
- Ensure staff are **appropriately educated and trained** so policies are effectively implemented, and staff are aware of the dangers of **unexpected invitations and links.**
- Protect calls with **strong passwords**.
- Consider using VCA **tools and security features** to ensure VCA sessions are secure and data protection compliant.
- **Be wary when screen sharing,** to ensure open documents, browser windows or desktop backgrounds are not visible.
- Use the **latest software versions** of VCAs and take greater care when **confidentiality is crucial**.

CONTENTS

1. ACKNOWLEDGEMENTS.....1
2. INTRODUCTION 2
3. GUIDANCE FOR INDIVIDUALS.....3
4. GUIDANCE FOR ORGANISATIONS.....6

1. ACKNOWLEDGEMENTS

Where appropriate the Information Commissioner will seek to ensure that locally published guidance notes are consistent with those published by fellow Information Commissioners in other jurisdictions.

As well as reflecting the existing data protection standards and practices in Gibraltar, parts of this document reflect and/or incorporate the guidance from the Irish Data Protection Commission, the UK's Information Commissioner's Office, the Office of the Privacy Commissioner of Canada and the Federal Trade Commissioner of the United States of America.

The following documents were used in the production of this Guidance Note:

(a) Ireland's Data Protection Commission

'Data Protection Tips for Video-conferencing'
https://www.dataprotection.ie/en/news-media/blogs/data-protection-tips-video-conferencing

(b) Information Commissioner's Office (UK)

'Blog: Video conferencing: what to watch out for'
https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/blog-video-conferencing-what-to-watch-out-for/

(c) Office of the Privacy Commissioner of Canada

'Privacy Tech-Know blog: Video conferencing – Maintain your physical distance, but keep your personal information close'

https://www.priv.gc.ca/en/blog/20200501/

(d) Federal Trade Commission – Protecting America's Consumers

'Video conferencing: 10 privacy tips for your business'
https://www.ftc.gov/news-events/blogs/business-blog/2020/04/video-conferencing-10-privacy-tips-your-business

2. INTRODUCTION

The COVID-19 pandemic has resulted in a sharp uptake in the use of Video Conferencing Applications ("VCAs").

In response to social distancing requirements, not only have individuals spent more of their social time at home, but remote working conditions have also been introduced by many organisations. This has contributed to a significant increase in the use of VCAs.

VCAs enable face-to-face communication between two or more individuals in different locations, offering both individuals and organisations an alternative, inexpensive means of communication.

The increased use of VCAs, however, introduces risks to privacy and to the protection of personal data. It is important that individual users are aware of and fully understand the data protection and privacy risks that exist when VCAs are used, as well as the steps they can take to protect their privacy. Organisations that implement the use of VCAs into their operational arrangements should also be aware of the risks to personal data and privacy and ensure that they adopt appropriate measures to protect individuals and their personal data.

In the following, the Information Commissioner's office provides guidance to -

- individuals on how to protect their personal data and privacy when using VCAs; and
- organisations on compliance with data protection legislation when using VCAs.

3. GUIDANCE FOR INDIVIDUALS

In the wake of the COVID-19 pandemic, technology is helping us all stay connected. Coping under such extraordinary circumstances may however lead individuals to prioritise convenience over security when using VCAs.

The Information Commissioner is aware of the increased risks to privacy posed by the use of VCAs and provides the following guidance for individuals:

(a) Research

Prior to the use of a VCA, it is recommended that individuals research the different services available so as to decide which one best suits their requirements. It is important for individuals to be aware of the data protection assurances provided by the operator of their chosen VCA. For example, individuals may wish to know whether a provider is operating their VCA platform in a secure manner and whether they are ensuring that personal data processed within said platform (e.g. any personal data submitted by users) is not being used or disseminated beyond the organisation.

Amongst other things, individuals should ask themselves the following questions –

- What categories of personal data is the VCA processing about me?
- How much personal data is being collected about me?
- Is my personal data being processed lawfully?
- Do I really need to share my location data or list of contacts with the VCA?
- How long is my personal data being retained for?
- Will my personal data be shared with third parties?
- Does the operator have a "Privacy Notice" that explains the above in a clear manner and that provides the contact details of their Data Protection/Privacy Officer?

(b) Ensure you are secure

When creating a new VCA account, it is advisable that individuals familiarise themselves with the security and/or privacy settings available. Take time to review the default settings applied to make sure you are satisfied with the standard security measures already in place.

(c) Password protection

In regard to account login and password, individuals should make every attempt to ensure their passwords are strong and unique by using a random string of uppercase and lowercase

letters, numbers, and symbols where possible. Passwords should not be written down and left in convenient places or shared with other individuals.

(d) Be private

When planning to host a video conferencing session, make sure that the session is only accessible to the targeted participants whom you have invited. Ensure each session is private, to prevent unwanted third parties joining.

Be mindful of the passwords you use when a video conference call or meeting is setup. Certain VCAs auto-generate a password in addition to a meeting ID number, but users may take precautionary measures and create a separate password or PIN where the platform allows.

Avoid publicly announcing the meeting ID and/or passwords on social media or other public forums for all to see and possibly access. Similarly, ask fellow participants not to share said information.

(e) Be savvy

When using VCAs, refrain from unnecessarily disclosing personal information. In regard to other participants, and where you are administrating the session, consider disabling the participants' abilities to screen share or actively record the session using video/camera or audio features.

If you are going to share your screen, be careful. Before sharing your screen, make sure you do not have open documents, browser windows, or other things on your screen you do not intend others to see.

(f) Surroundings

Ensure that your surroundings, as captured via the webcam during a video conference, do not reveal information that you might not want to share with others. Likewise, turning off your webcam and listening in via audio only, prevents possible social engineering efforts to learn more about you through background objects.

Alternatively, several VCA platforms provide additional features so that individuals can for example apply virtual backgrounds to prevent their surroundings from revealing too much information about them.

If there are others around, individuals are also encouraged to move to a different room or use headphones to prevent such persons from listening in.

(g) Keep yourself updated

Be sure to use the latest versions of VCA software as security vulnerabilities are likely to be exploited more often on older software versions. It is advisable that individuals, where possible, select auto-updates for the software. If the VCA platform does not allow for this, it

is important that individuals make it a habit to regularly check for and apply the available updates.

Double-check in advance that joining participants are also using the most up-to-date version available to ensure utmost security and to also reduce any compatibility issues.

(h) Be considerate

Consider the data protection and privacy rights of other participants before you post or share information, be it a picture, transcript or video that contains someone else's image, voice and/or contact details for example.

(i) Browsers

If you are using a web browser for the video call, it would be best to open a new window with no other browser tabs. Preferably, close other applications to avoid inadvertently sharing notification pop-ups (e.g. new incoming emails) with other participants and the video conferencing service provider.

(j) Smart speakers

If you have a smart speaker or personal home assistant (Alexa, Siri, Google Home, etc.), consider turning it off during your video conference. This will help prevent you from accidentally triggering the assistant and/or recording your call.

(k) Default access to audio and video

When you join a meeting, your video camera and microphone may be on by default. If you don't want to share sound or video, most services allow you to mute yourself or turn off your camera. You may be able to adjust the default settings so your preferences are stored for the next meeting or, depending on the service, you may need to adjust your settings at the beginning of each call.

(l) Recording

Check to see if your video conference is being recorded. The service should display some indicator to advise that you're being recorded – for example, a bright red circle or the word "recording." But remember that a meeting may be recorded even if these indicators don't appear. The safest strategy is to assume you might be recorded and, if possible, avoid sharing private information via video conference.

(m) Unexpected invitations and links

Don't open unexpected video conference invitations or click on unexpected links. With the upsurge in video conferencing, malicious actors are sending emails mimicking meeting invitations or other communications from video conferencing services. To add authenticity, they may copy the logo and look of familiar names in the business. But instead of taking you to a video conference, those links may contain viruses or install malware on your computer. The safer practice is to only accept invitations to teleconferences that are planned and agreed for a certain date and time in advance. Unexpected invitations and links should not be opened.

If the service you're using requires you to download an app or desktop application, make sure you download it directly from the service's website or a platform's app store

4. GUIDANCE FOR ORGANISATIONS

VCAs offer organisations an inexpensive, alternative means of communication, which in recent months appears to have substantially substituted the former, more traditional method of telephone conferencing.

The increased use of VCAs has led to the rapid development of such platforms, which include an array of services for organisations to choose from. Many organisations are therefore turning to VCAs to ensure their operations continue to run smoothly. Organisations need to carefully consider the privacy and data protection implications of using VCAs.

The guidance provided to individuals in section 3 may also be relevant when VCAs are used by an organisation's employees and should therefore also be considered by organisations. The Information Commissioner provides the following further guidance for organisations:

(a) Business needs

In line with an organisation's data protection responsibilities and obligations under the GDPR and DPA, organisations should consider the implications of their use of VCAs and their compliance with data protection.

Organisations are advised to acquaint themselves with the different types of VCAs available and consider their features from a data protection perspective before choosing the one best suited to the organisation's needs.

Articles 5(2) and 24 of the GDPR emphasise the accountability of data controllers when processing personal data[1]. Organisations subject to the GDPR should therefore ensure they are able to demonstrate that they have taken relevant considerations and implemented appropriate measures to ensure the compliant and safe use of VCAs.

[1] For processing under Part III of the DPA, see sections 43(3) and 65 of the DPA.

(b) Data protection principles and organisational security

It is important to note that the seven foundational principles as set out in Article 5 of the GDPR are intended to embody the standards that organisations are bound to in respect of the processing of personal data[2]. Of particular importance, is Article 5(1)(f) of the GDPR, which requires organisations to use "*appropriate technical or organisational measures*" to process personal data in a manner that "*ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing*" as well as "*accidental loss, destruction or damage*"[3].

The "*appropriate technical and organisational measures*" can be understood to include maintaining relevant data protection policies and taking steps to make sure that policies are executed accordingly (as advised in points c and e below), which in turn, would also ensure compliance with the accountability principle[4].

A well-meaning staff member may inadvertently put sensitive personal data at risk by enabling VCAs that do not meet your organisation's data protection or security standards. It is therefore important to establish organisation-wide VCA do's and don'ts, and emphasise the need to select the more secure options when hosting or joining sessions.

(c) Policy

Article 24(2) of the GDPR explicitly says that, where proportionate, implementing data protection policies is one of the measures that can be adopted to ensure and demonstrate compliance with the GDPR[5]. Organisations should therefore consider establishing their own policies and/or procedures so that their staff only use VCAs in a data protection compliant manner. Said policies and/or procedures should be clear, understandable, and up to date.

For policies to be effectively implemented in practice, staff need to be informed and trained in these as appropriate.

(d) Transparency and fairness

Transparency and fairness[6] are key GDPR requirements, which organisations should consider in situations when they use VCAs. In particular, organisations should be transparent about any monitoring of staff use and/or activity.

It is important that all staff are made aware of how their privacy and data protection rights may be affected, and why the monitoring, if applicable, is necessary (i.e. to protect the

[2] For processing under Part III of the DPA, see sections 43 to 49 of the DPA.

[3] For processing under Part III of the DPA, see section 49 of the DPA.

[4] Article 5(2) of the GDPR says: "*The controller shall be responsible for, and be able to demonstrate compliance with paragraph 1 [the other data protection principles]".* For processing under Part III of the DPA, see section 43(3) of the DPA.

[5] For processing under Part III of the DPA, see section 65 of the DPA.

[6] See Articles 5(1)(a) and 13 of the GDPR. For processing under Part III of the DPA, see sections 44 and 53 of the DPA.

personal data of staff and customers alike, as well as confidential information belonging to the organisation).

(e) Staff training and education

As noted in the foregoing, the education and training of staff is important to ensure policies are effectively implemented in practice. For example, staff should be trained and educated on the security measures adopted by the organisation to ensure the integrity and confidentiality of personal data (i.e. Article 5(1)(f) of the GDPR) when using VCAs. Well-designed security measures will not work if staff do not know about or follow the organisation's related policies and/or procedures. These should be made available to all staff and may for example be promoted via staff intranet pages, policy libraries or through leaflets and posters.

Organisations should educate staff on the appropriate use of security controls, such as access controls[7], and inform them that they should limit use and data sharing to what is necessary, more so, if it involves special categories of personal data.

Organisations may not always be able to take a blanket approach and it may be necessary to consider, and thereafter educate, individuals separately or as part of a specific group/team, depending on the categories of personal data likely to be exposed through the organisation's use of VCAs.

(f) Unexpected invitations and links

Unexpected invitations and links are already mentioned in section 3(m) above. Staff should be briefed and provided with adequate training to identify "real" video conference invitations from reliable sources, to avoid clicking on a link which may contain viruses or install malware on the device being used.

Safe practice dictates that organisations should warn their staff in advance about any planned video conference call and make them aware that an invitation will be sent to them within a specified timeframe. Such procedure would also assist organisations to evidence their implementation of appropriate technical and organisational measures as required by the GDPR when processing personal data.

(g) Passwords

Protect your video conferencing calls with a password, especially if you intend to discuss sensitive personal information such as health information. Each call should have its own password to prevent any unwanted participants from joining.

(h) In-app security features

Organisations should take advantage of the tools at their disposal to ensure VCA sessions are secure and data protection compliant.

[7] Refer to section 5.2.1 of the Information Commissioner's Guidance Note on Data Security.

Amongst other things, organisations may consider access controls[8] whereby the host locks the meeting once the expected participants have joined, or enables settings to allow the host to approve each and every participant trying to join. Likewise, the host may be afforded the ability to remove individual users from the meeting should the need arise. Such mechanisms would assist in ensuring that personal data is only disseminated to necessary persons and protected from unlawful disclosure.

(i) Screen sharing

Organisations may deem the use of screen sharing to be essential in facilitating workflow and efficiency. Before doing so however, staff members should be aware that open documents, browser windows, desktop backgrounds or icons may be viewed by others when not intended, potentially in breach of the GDPR and/or the DPA. Certain VCAs have options that allow the host to turn off screen sharing or to limit its use to the host, which should also be considered by the relevant organisation.

(j) Updated software

The more reputable VCA providers continually monitor their systems and thereby learn about vulnerabilities, allowing them to adapt and update their software to implement appropriate technical and organisational security measures. It is important that organisations use the latest software versions of VCAs as these updates are important to the safety and security of the personal data processed using these platforms. Software updates help protect data by helping to keep malicious actors away, but may also add new features and improve existing ones.

Organisations should also ensure that the relevant updates are only processed by staff with specific security responsibilities or with privileged access to business systems and, that said updates are only accepted from the VCA's primary website[9].

(k) Confidentiality

Take greater care when confidentiality is crucial. It is likely that paid for VCA services are more suitable or it may be that the use of VCAs may not be appropriate to the relevant processing of personal data. Ultimately, organisations should make efforts to guarantee the security of the personal data being processed, particularly when sensitive topics need to be discussed.

[8] Refer to section 5.2.1 of the Information Commissioner's Guidance Note on Data Security.
[9] Refer to section 5.2.4 of the Information Commissioner's Guidance Note on Data Security.

IMPORTANT NOTE

This document is purely for guidance and does not constitute legal advice or legal analysis. All organisations that process personal data need to be aware that the GDPR and the DPA may apply directly to them. The responsibility to become familiar with the GDPR and the DPA and comply with its provisions where applicable lies with the organisation.

Where necessary, the Information Commissioner will review this Guidance Note in accordance with any updates or other developments. In the event of any conflict or inconsistencies between this Guidance Note and the GDPR and the DPA, the GDPR and the DPA will take precedence.

CONTACT US

Gibraltar Regulatory Authority
2nd floor, Eurotowers 4, 1 Europort Road, Gibraltar

(+350) 20074636
privacy@gra.gi
www.gra.gi