21/07/2020

GIBRALTAR REGULATORY AUTHORITY

2nd Floor, Eurotowers 4
1 Europort Road
Gibraltar

Tel: +350 20074636
E-mail: privacy@gra.gi

PRESS RELEASE

GLOBAL PRIVACY EXPECTATIONS OF VIDEO TELECONFERENCE PROVIDERS

The Gibraltar Regulatory Authority, alongside other data protection and privacy authorities from around the world, has today published an open letter to video teleconferencing companies, reminding them of their data protection obligations. The Covid-19 pandemic has resulted in a sharp uptake in the use of video teleconferencing software, increasing risks around the collection and use of personal information. The open letter provides video teleconferencing companies with principles to help them identify and address some of the key privacy risks, and better protect people's personal information.

The open letter is signed by six authorities brought together through the Global Privacy Assembly's International Enforcement Cooperation Working Group. The six authorities are the Gibraltar Regulatory Authority as Information Commissioner, the Office of the Australian Information Commissioner, the Office of the Privacy Commissioner of Canada, the Hong Kong Privacy Commissioner for Personal Data, the Switzerland Federal Data Protection and Information Commissioner and the UK Information Commissioner's Office.

The letter is intended for all video conferencing companies, but has also been sent directly to Microsoft, Cisco, Zoom, House Party and Google. A copy of the letter is available at Annex A.

For further information, please contact the Gibraltar Regulatory Authority on +350 200 74636 or email: privacy@gra.gi.

Annex A

Joint statement on global privacy expectations of Video Teleconferencing companies

Introduction

This is an open letter to companies providing Video Teleconferencing (VTC) services. We write to you as a subset of the global privacy regulatory community, with responsibility for protecting the privacy rights of citizens across the world.

Privacy concerns

Use of VTC to stay connected is not new. But as a result of the Covid-19 pandemic, we have seen a sharp increase in the use of VTC for both social and business purposes, including in the realm of virtual health and education, which can involve the sharing of particularly sensitive information, for particularly vulnerable groups. This increase in use exacerbates existing risks with the handling of personal information by VTC companies, and also creates new ones.

Reports in the media, and directly to us as privacy enforcement authorities, indicate the realisation of these risks in some cases. This has given us cause for concern as to whether the safeguards and measures put in place by VTC companies are keeping pace with the rapidly increasing risk profile of the personal information they process.

This letter

The purpose of this open letter is to set out our concerns, and to clarify our expectations and the steps you should be taking as VTC companies to mitigate the identified risks and ultimately ensure that our citizens' personal information is safeguarded in line with public expectations and protected from any harm.

Note that this is a non-exhaustive list of the data protection and privacy issues associated with VTC. It is intended to remind you of some of the key areas to consider given the increased use of your VTC services.

You should still regularly review your thinking on key privacy questions through privacy impact assessments. Where risks cannot be mitigated, we expect organisations to consult with their privacy

regulator(s) to explain the specific risks identified and work through possible solutions on how these might be addressed.

Principles

1. Security

With personal information driving our digital economies, cyber-risks and threats to data-security are in a constant state of morphing and evolution. Today's security measures may soon become outdated and compromised by emerging threats. Data-security is a dynamic responsibility and vigilance by organizations is paramount.

During the current pandemic we have observed some worrying reports of security flaws in VTC products purportedly leading to unauthorised access to accounts, shared files, and calls.

In a world of global conversations, with personal information and private communications passing through many countries, we believe VTC providers should have certain security safeguards in place as standard, which would generally include: effective end-to-end encryption for all data communicated, two-factor authentication and strong passwords.

Such security measures should be given extra consideration by organisations who provide VTC services for sectors that routinely process sensitive information, such as hospitals providing remote medical consultations and online therapists, or where the VTC platform allows sharing of files and other media, in addition to the video/audio feed.

Your organisation should remain constantly aware of new security risks and threats to the VTC platform and be agile in your response to them. We would anticipate that you routinely require users of your platform to upgrade the version of the app they have installed, to ensure that they are up-to-date with the latest patches and security upgrades.

Particular attention should also be paid to ensuring that information is adequately protected when processed by third-parties, including in other countries.

2. Privacy-by-design and default

If data protection and privacy are merely afterthoughts in the design and user experience of a VTC platform, it increases the likelihood that you may fall short of the expectations of your users in upholding their

rights. For instance, we have seen this manifest itself in well documented accounts of unexpected third-party intrusion to calls.

You should ensure that you take a privacy-by-design approach to your VTC service. This means making data protection and privacy integral to the services you provide to the customer. Always consider, as a starting point, the most sensitive information that could potentially be shared on your platform, and adopt the most privacy-friendly settings as default (similar to the **principle of least privilege** in cyber security). People who use your platform for less sensitive conversations or content sharing can adjust these settings to suit their requirements.

Simple measures to achieve this include:

- creating privacy conscious default settings that are prominent and easy to use, including implementing strong access controls as default, clearly announcing new callers, and setting their video / audio feeds as mute on entry;

- implementing features that allow business users to comply with their own privacy obligations, including features that enable them to seek other users' consent; and

- minimising personal information or data captured, used and disclosed by your product to only that necessary to provide the service.

VTC providers should also undertake a privacy impact assessment to identify the impact of their personal information handling practices on the privacy of individuals, and implement strategies to manage, minimise or eliminate, these risks.

3. Know your audience

During the Covid-19 pandemic, we have seen many examples of VTC platforms being deployed in contexts for which they were not originally designed. This can create new risks that you may not have anticipated prior to the current crisis.

Therefore, make sure that you review and determine the new and different environments and users of your VTC platform as a result of the pandemic. This is particularly important when it comes to children, vulnerable groups, and contexts where discussions on calls are likely to be especially sensitive (in education and healthcare for example), or when operating in jurisdictions where human rights and

civil liberty issues might create additional risk to individuals engaging with the platform.

Consider what the data protection and privacy and requirements are for *all* contexts in which your platform is now in use, and implement appropriate measures and safeguards accordingly.

4. Transparency and fairness

As a result of several high-profile privacy breaches over recent years, there is heightened community awareness and expectations regarding how organisations handle personal information and use data in today's global digital economy. This is no different when it comes to VTC platforms. Failing to tell people how you use their information, and not considering whether what you are doing is expected and fair, may lead to a violation of the law and of the trust of your users.

You should be up-front about what information you collect, how you use it, who you share it with (including processors in other countries), and why – even if you do not consider the collection, use or sharing of that information to be particularly significant yourself, it is still important that its use is honestly communicated to the customer at all times. This is particularly the case when what you do with people's information is unlikely to be expected because it would not be seen as a core purpose of the VTC service. This information should be provided pro-actively, be easily accessible and not simply buried in a privacy policy. Where user consent regarding the handling of personal information is required, you should ensure that such consent is specific and informed.

Consider how any changes you make to future versions of the platform will affect all of the above. Assess their impact and consider whether it is important to make users aware of these changes. This will allow them to make informed decisions about how they use your platform moving forward.

5. End-user control

End-users may often have little choice about the use of a VTC service if a particular platform has been purchased, or is being exclusively utilised, in a given work-place, school or other setting. Some of the more novel features of VTC platforms may raise the risk of covert or unexpected monitoring.

While the companies and institutions using your VTC platform have their own data protection, privacy, and broader legal and ethical considerations in making decisions about the use of monitoring features, you should take your own steps to ensure that end-users of your service are empowered by having appropriate information and control.

For instance, if you offer a VTC platform that allows the host to collect location data, track the engagement or attention of participants, or record or create transcripts of calls, you should ensure that the use of these features is clearly indicated to those on the call when they are activated (through icons and pop-ups, for example). Where possible, you should also include a mechanism for end-users to choose not to share that information, for example via opt-out, noting that opt-in mechanisms might be more appropriate in certain instances.

Summary

We recognise that VTC companies offer a valuable service allowing us all to stay connected regardless of where we are in the world; something that is especially important in the midst of the current Covid-19 pandemic. But ease of staying in touch must not come at the expense of people's data protection and privacy rights.

The principles in this open letter set out some of the key areas to focus on to ensure that your VTC offering is not only compliant with data protection and privacy law around the world, but also helps build the trust and confidence of your userbase.

We welcome responses to this open letter from VTC companies, by 30 September 2020, to demonstrate how they are taking these principles into account in the design and delivery of their services. Responses will be shared amongst the joint signatories to this letter.

Elizabeth Hampton
Deputy Commissioner
Office of the Australian Information Commissioner
AUSTRALIA

Brent R. Homan
Deputy Commissioner
Compliance Sector
Office of the Privacy Commissioner of Canada
CANADA

Paul Canessa
Information Commissioner
Gibraltar Regulatory Authority
GIBRALTAR

Stephen Kai-yi Wong
Privacy Commissioner for Personal Data
HONG KONG, CHINA

Adrian Lobsiger
Federal Data Protection and Information Commissioner
SWITZERLAND

James Dipple-Johnstone
Deputy Commissioner
Regulatory Supervision
Information Commissioner's Office
UNITED KINGDOM