SAFE USE OF VIDEOCONFERENCING

URZĄD OCHRONY DANYCH OSOBOWYCH

New technologies have opened up completely new opportunities. Video conferencing and¬ video calls are among the most popular ways of communication at the time of teleworking and online contacts with friends and family resulting from the current situation connected with reducing the spread of COVID-19.

This raises concerns about how to safely use the wide range of programmes, applications and services offered, and how to ensure that this form of contacts ensures an adequate level of protection of personal data.

The Personal Data Protection Office (UODO) suggests how to use videoconferencing in a safe way.

Before starting a videoconference

1. Read the general terms and conditions or privacy policy of the programme which you wish to use.

2. Check whether your calls will be recorded and stored.

3. Verify the purposes for which your personal data will be used.

4. Check what data use permissions you are asked for – contact list, location, etc.

5. Use the official website of the application that you want to use for the purpose of installing the application on your computer; for mobile devices, select an official store – Google Play or App Store.

6. Make sure that bystanders do not have access to your screen.

7. Check whether the application has the necessary security measures, such as encryption.

8. Use web applications, not desktop applications.

9. Secure the Wi-Fi network with a strong password.

10. Before sharing your screen during a conversation close all windows, so that other conference participants do not see them.

11. When connecting to a teleconference, use the access codes/PIN codes.

12. Scan the teleconferencing programme with your antivirus or antimalware system.

During the use of videoconferencing

1. Limit the amount of personal data provided – use a pseudonym and business e-mail address.

2. Use a different password than the one used by you in other services.

3. Do not share links to conferences on social media.

4. Enable, if possible, the default password protection of the online meeting.

5. Manage screen sharing options.

6. Use network access via an encrypted VPN connection to make business calls.

7. Do not share official documents, via chat, which may be public.

8. If possible, use the background blur option (so that the callers do not see your surroundings)).

9. Use the “waiting room” option, so that you can control the persons participating in a teleconference, which allows you to avoid accidental or unwanted participants.

10. When logging in to the teleconference, turn off the microphone and the camera (you will turn them on if needed).

After using videoconferencing

1. Turn off the microphone and the camera.

2. Make sure that you have terminated the online meeting and closed the application.

3. Check whether the teleconferencing programme is not working in the background.