Web Camera Usage & Privacy

Ver. 22-Jul-2021

Is using the Seebird remote inspection and support system considered surveillance in Norway?

The short answer is no.

According to Norwegian law, a surveillance system is defined as *"camera surveillance meant for continuous or regularly repeated personal surveillance by means of a remote-controlled or automatic-acting surveillance camera or other similar equipment that is permanently mounted."* Read more; www.lovdata.no/dokument/SF/forskrift/2018-07-02-1107 (in Norwegian language only).

The Seebird system avoids falling under the Norwegian legal definition of camera surveillance in the following ways:

1. Our PTZ web camera is not mounted as it is designed to be set up and taken down from a portable, temporary tripod.
2. The software is designed with movement limitations that limit what remote viewers can observe. The host has total control in restricting what can be viewed at any time eliminating the risk of capturing personal details and instead focus on the product being tested, inspected, or repaired.
3. The software has programmable pre-sets that allow the camera to snap to points of interest, avoiding the need for scanning and observing unnecessary or personal details.
4. The host of the session always has complete control over who is viewing the camera feed and if/when the session starts or ends. The host also has complete control over the video and audio feed and can disconnect either or both at any time. This allows the host to avoid regular or repeated personal surveillance entirely.
5. The system is designed specifically for quality inspections, technical support and training, not for personal surveillance. By requiring the licensed host to initiate a session, the host is fully aware of the camera and the video stream and can eject attendees from the session at any time. This allows the host autonomous control of the session and environment that the camera can capture.
6. Identifying information associated with the video session is solely under the control of participants who were in the session. This includes session receipts and screen shots. The host and attendees can choose to delete this information at any time and information that cannot be deleted is presented in an anonymized way. Seebird has access to more information, however this is only used for the purpose of providing the service to the license holders and will not be released or used for surveillance. See the End-User License Agreement (EULA) for details.
7. The video feed and information are not streamed online nor is any of the information available to anyone but the host and clients who the host has specifically invited. More information about webcam usage; www.datatilsynet.no/personvern-pa-ulike-omrader/overvaking-og-sporing/kameraovervaking/?id=2090 (in Norwegian language only).

Is using the Seebird remote inspection and support system considered surveillance according to European Union (EU)?

The short answer is no.

According to EU definitions, a VSS (video surveillance system) consists of three components: video environment, system management and system security.

The system management component must have data management and activity management, which includes handling operator commands and system generated activities (alarm procedures, alerting operators). It must also interface with other systems that might include connection to other security (access control, fire alarm) and non-security systems (building management systems, automatic license plate recognition). The Seebird inspection system does not have system generated activities such as alarm procedures, nor does it connect to other systems, therefore it does not fall under the definition of a surveillance system according to the current EU definition of a VSS. Read more; https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-32019-processing-personal-data-through-video_en

How can I be sure we comply with the law regarding the use of cameras in the workplace?

Seebird utilizes USB cameras that plug into a laptop that are comparable to a webcam mounted to a PC or the webcam in a laptop used for meetings. Your IT department will likely have policies in place for responsible use of web cameras, especially if web conferencing software is in use within your company. Seebird systems are designed to reduce the need for travel and meeting in person for the sake of quality inspections and technical support/training and therefore fall under the same guidelines as online meetings.

We urge all customers to familiarize themselves with the applicable laws of their country. Nevertheless, we can recommend a number of best practices to make implementation smoother:

1. Your company should have a legitimate need for using the system and it cannot be for monitoring personnel.
2. Only view and capture data related to that legitimate need.
3. Ensure that there is sufficient visible signage about the activity that indicates the following;
    - When the video inspection will occur.
    - Where inspection will occur through placement of the signage.
    - Who the site representative/responsible is and how they can be contacted.
    - Printable sign for lamination can be found here; http://inspection-sign.seebird.no/
4. Have your site representative/responsible familiarize themselves with the applicable legislation and laws to eliminate confusion and misinformation that can circulate.
5. Set the limits in the Seebird software to restrict unwanted viewing of the workplace.
6. Before a license is assigned, ensure that the assignee understands what the system is and the features that allow them to limit unwanted intrusion into their privacy. The assignee should be a willing participant in the use of the system.
7. If streaming from a mobile camera, drone, ROV, or similar, ensure that the privacy of those on site is respected and maintained – activities should be restricted to the environment and time indicated in site communications and signage.
8. To ensure all are informed, include information regarding remote inspection systems in your company's induction information package for all employees, contractors and guests to avoid confusion.

Are the following measures necessary when using the Seebird system?

1. **Blurring or masking the face**: If you are not required to blur and mask people's faces when using your company conferencing systems, then you should not be required to do this with the Seebird system as it does not meet the Norwegian or EU definition of a VSS.
2. **Setting up of physical barriers where inspection and support activities will be conducted**: If you are not required to have physical barriers when using your company conferencing systems, webcams and mobile phone cameras, then you should not be required to do this when using Seebird systems.
3. **Acquiring specific legal approval every time you plan to use the Seebird system**: Since the system is only designed for internally approved use between informed and consenting parties and not for public streaming, additional legal approval should not be required. If you do not require specific approval when using your company's online conferencing systems, then you should not require specific approval for using Seebird systems.
4. **Designation of a data protection officer**: Article 37 (1) (b) in GDPR requires data processors to designate a data protection officer, if the processing operation by its nature entails regular and systematic monitoring of data subjects (people). This system is specifically designed with measures to prevent the monitoring of people as subjects. It is intended and designed for the inspection of equipment and associated technical support and testing and therefore does not require a data protection officer. Read more; www.gdpr-info.eu/art-37-gdpr
5. **Right to access data**: Since images and video captured are not searchable based on personal data, identifying someone by searching the data is not possible. If a request for access is submitted, the requestor must provide identification and a specific timeframe when they entered the equipment inspection or test area. In cases of excessive or unfounded requests, the controller may charge a reasonable fee in accordance with GDPR Article 12 (5) (a) or refuse to act on the request Article 12 (5) (b). Read more; www.gdpr-info.eu/art-12-gdpr
6. **First and second layer information**: Since no personal data relating to a data subject (person) is collected, there is no legal requirement within the EU to provide additional information about the inspection activity. Read more; www.gdpr-info.eu/art-13-gdpr

Additional information can be found here:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
https://www.lovdata.no/dokument/SF/forskrift/2018-07-02-1107 (in Norwegian language only)