

New legal regulations for CCTV in Austria

The amendment of the Austrian Act on Data Protection, which came into effect in January 2010, created a (more or less) clear fundament for CCTV in Austria for the first time. Operators of the numerous already existing CCTV systems should urgently verify whether their systems comply with the new regulations. Likewise, everybody who intends to build new CCTV systems must consider the new regulations in time. Anyone who fails to do so not only risks substantial fines but perhaps the prohibition of further use of the CCTV system and therefore the loss of all investments made.

What is "Closed Circuit Television" within the meaning of the law?

The Austrian Act on Data Protection conceives of CCTV as

- systematic, especially continuous, observation of events
- which concerns a certain object or a certain person,
- through technical image recording or image transmission devices.

Therefore, not only the recording and storage of image files, but even the mere real-time transmission (e.g. to a porter or a central surveillance point) or the systematic, that is recurrent, production of photo images of the same object (e.g. to check whether the maximum parking duration was exceeded on a super market parking lot) is subject to these provisions. For real time coverage there are some alleviations in regard to particular formal requirements.

When is CCTV permitted?

According to the law, CCTV is **permitted exclusively to serve the purpose of protecting the monitored object or person as well as the compliance of other duties of care subject to the law** (e.g. traffic control). Many existing facilities, which serve other purposes (e.g. web cams) stand - given the image resolution is high enough to identify persons distinctly- on shaky legal ground.

Even within the protection purpose CCTV may only take place if

- it is convened in real time (without the storage of images) for the sake of protection of body, life or property of the controller, or
- there is any reason to believe that a dangerous attack on the monitored building or person could occur (e.g. because such attacks like thefts or acts of vandalism etc. have already occurred or are expected to due to the valuables on hand (bank, jeweler, etc.) or the position of the monitored person), or
- the affected persons explicitly agree to the CCTV activity.

When is CCTV still forbidden?

Even if all the aforementioned criteria apply, CCTV is not permitted if the intended purpose could be reached through other reasonable means, which interfere with the person's private sphere to a lesser extent as CCTV.

CCTV is absolutely forbidden at places which are rated among the most personal spheres of affected persons such as toilets and changing rooms.

What should employers, who intend to use CCTV, bear in mind?

On no account must CCTV be used as a means of control of employees! This also applies to real time CCTV. This ban cannot be circumvented by consent of the employees e.g. in the labour contract.

In the case of an existing employee organization, it must be informed about the planned introduction of a CCTV system. Is the system suited to "affect human dignity" (which can be difficult to discern in individual cases), the additional conclusion of a company agreement is required.

If no employee organization exists, individual agreements must be concluded with every single employee.

Which formal provisions must be observed?

The intended CCTV must be notified to the Data Protection Authority before (!) its activation. The activation may only take place after the permission of the Authority, or if the Authority does not react, two months after the announcement.

Not subject to announcement to the Authority are facilities which merely serve the purpose of real time coverage or store the data on analogue media (e.g. VCR tapes).

The CCTV must be indicated noticeably! If possible, this must be done in a manner which enables the affected person to elude the CCTV before entering its range. Due to the labelling (usually done through clearly visible symbols) it must be made clear (if this is not clear already due to the circumstances of the individual case) who the controller of the system is.

All recordings must be **erased within 72 hours**, provided the Data Protection Authority has not exceptionally granted a longer deadline. Only those recordings, which contain concrete incidents within the scope of the protective purpose and are therefore being forwarded to the authorities, as well as those recordings, for which a right to information was claimed by the affected person, may be stored until the completion of these purposes.

Information rights of the affected persons

Each person, who may have been affected of such surveillance, can- after proof of identity and indication of the approximate time and place of the recording- claim the inspection of the data or the issuance of a copy of the recording from the controller of the CCTV on commercially available data carriers. This has to be done for free once a year, in case of repeated inquiries an appropriate reimbursement of costs must be rendered. Naturally such an obligation only exists if the inquiry reaches the controller before the data was erased (usually after 72 hours). The controller must also announce the origin of the data, its purpose and the legal foundation upon which the data was collected and if necessary the consulted service contractor.

Would the disclosure of the recorded images predominantly affect justified interests of third parties (e.g. other persons, which were also recorded), the controller has to, instead of handing over of a copy, give the inquiring affected person a written description of the person's activities covered on the recording.

No automatic image comparison

Any automatic comparison of the images gained by CCTV with other digital image-files is explicitly forbidden!

Logging of every data usage

Any usage of the recorded data – such as the review of recordings, any evaluation and transfer to third parties - must be instantly logged by the controller, so that it is possible to reconstruct even after the erasure of the data, in which way they were used.

What must be considered with CCTV systems already authorised?

In the case that systems were authorised (without any time limitation) by the Data Protection Authority before said amendment of the law came into effect, the operation of the systems may continue as before. However, the new regulations such as the prohibition of the usage of CCTV for the control of employees, the information rights or the obligation to log any usage of the recordings must be followed as of now.