Privacy Interviews with Experts
June 2015

Rainer Knyrim
Attorney at Law
Preslmayr
Vienna, Austria

Austrian Court limits individuals' right of access to CCTV footage

A recent case in Austria's Administrative Court dealt with an individual's appeal of the Data Protection Authority's (the "DPA") decision denying the individual access to closed-circuit televisions system ("CCTV") footage. Rainer Knyrim, Attorney at Law and Partner, Preslmayr Attorneys at Law, discusses this case and on what basis it was determined the individual did not have a right to such access, and provides guidance on what organisations should consider when implementing CCTV systems.

Rainer studied law in Vienna, Graz and Paris. Author of numerous privacy related publications, chief editor of the Austrian privacy law journal "DAKO" (data protection concrete), Rainer was one of the first certified experts for the European Privacy Seal EuroPriSe, is member of the "Privacy Task Force" of the ICC in Paris, member of the scientific committee of a legal review on IT and data protection law and member of the advisory board of the Austria IT Law Symposium and Certified Information Privacy Manager (CIPM).

Nymity: This case dealt with an individual's right to access CCTV footage. What rights of access to personal data are included in Austria's data protection law and what obligations does this confer on data controllers?

Knyrim: Basically the right of access is already included in the fundamental right to privacy. This constitutional law is specified in detail in the Austrian Data Protection Act (ADPA). Due to the right of access persons have the right to demand from controller's information about all data they process of them including information to the origin of the data and possible recipients of data transmissions. Upon receiving a request for information from a person, controllers must handle the request within eight weeks. In the case, that a controller does not process data to an individual, the controller must inform the individual about that fact and provide a so called "negative information". Once per year controllers must deal with requests for information from a specific individual free of charge. Only for additional requests for information controllers may charge compensation for it's expenses.

Nymity: Does data protection law, or any other statute in Austria, specifically address the use of CCTV, including the right of access to CCTV footage?

Knyrim: In 2010 the ADPA was revised in order to explicitly regulate CCTV systems. A new provision was inserted into the ADPA amending the right of access regarding CCTV footage. The clause states, that, if a person files a request for information regarding CCTV footage, information must primarily be provided by sending the data subject a copy of the CCTV footage. Alternatively, if the transmission of a copy of the CCTV footage may harm the right to privacy of other persons, the controller can provide a written

report of the behavior of the data subject or a copy of the CCTV footage where all other persons (besides the one that requested the information) are technically made unrecognizable.

Nymity: What was the data controller's response to the individual's request for access? Did they provide a legal basis for that decision?

Knyrim: Upon receiving a request for information, the controller responded by writing the individual that – according to its opinion – there is no right for access as long as CCTV footage has not been "evaluated". As a legal basis for its legal opinion, the controller referred to decisions of the DPA that were issued prior the change of law in 2010 and were in accordance with the legal opinion of the controller.

Nymity: How did the DPA respond to the individual's complaint about the data controller's response?

Knyrim: Even though the ADPA has changed and contains specific regulations about how controllers have to deal with the right of access regarding CCTV footage, the DPA stated, that the new regulations merely amend the general right of access. Therefore the DPA was of the opinion, that their decisions issued prior the change of the law were still applicable and there is no right to access to CCTV footage as long as it has not been evaluated by the controller.

Nymity: What was the issue before the Administrative Court and how did the Court rule in this matter?

Knyrim: The issue was, whether an individual has a right of access to CCTV footage even if a controller has not evaluated the material due to an incident (e.g. a theft or a damage of property). The Court confirmed the decision of the DPA and ruled surprisingly, that as long as the CCTV footage has not been evaluated, no data is processed to individuals at all. Hence, there is no right of access regarding this data.

Nymity: What is the implication of the Administrative Court's decision for other data controllers who make use of CCTV in their premises?

Knyrim: For controllers, the decision of the Administrative Court means, that as long as they did not evaluate their CCTV footage due to an incident, they must only provide persons, who make use of their right for information, with a negative information. This is a major easement compared to the time consuming and costly process of having to provide a copy of the CCTV footage or a written report.

Nymity: Many organisations have installed or are considering installing CCTV systems – what are the top 5 key things organisations must consider and put in place to ensure that such systems meet the requirements of data protection law?

Knyrim: At first it must be considered whether a CCTV installation suits the needs of the organisation and whether it is the least intrusive method to archive the desired purpose. Secondly, an organisation must ensure that a CCTV system is only used for a legitimate purpose (protection of the object or the person observed or the fulfilment of legal duties of diligence, including securing of evidence). Thirdly, an organisation must check whether a works council agreement is necessary and if so whether an agreement can be obtained. Fourthly, an organisation must file a notification of the CCTV system with the DPA (the notification must include a description of the system, maps with the location of the cameras, a sample of the mandatory information signs used and, if applicable, a copy of the works council agreement) and must wait until the system is being registered by the DPA (this process can take up to six months) prior setting the system into use. Lastly, an organisation must ensure that the CCTV system is only conducted as registered. Any alterations of the system must be notified to the DPA and registered by it before they may be implemented.