EUROPÄISCHER RECHNUNGSHOF
Generalsekretariat

Europäischer Rechnungshof

Informationssicherheit

Faltblatt Videoüberwachungsstrategie

1. EINLEITUNG

Für die Sicherheit seiner Gebäude, Vermögenswerte, Mitarbeiter und Besucher betreibt der Europäische Rechnungshof (EuRH) ein Videoüberwachungssystem. Die vollständige Videoüberwachungsstrategie ist im Internet abrufbar unter eca.europa.eu/CCTV.

2. GEWÄHRLEISTUNG EINER EFFIZIENTEN UND ZIELGERICHTETEN VIDEOÜBERWACHUNG

2.1. Überprüfung des bestehenden Systems

Das Videoüberwachungssystem steht im Einklang mit den Leitlinien zur Videoüberwachung, die der Europäische Datenschutzbeauftragte am 17.3.2010 veröffentlicht hat („Leitlinien“).

Die CNDP (Commission Nationale pour la Protection des Données) als zuständige Datenschutzbehörde in Luxemburg wurde unterrichtet. Der Hinweis vor Ort und die Videoüberwachungsstrategie liegen insbesondere auch in französischer und deutscher Sprache vor.

2.2. Technologische „privatsphärenfreundliche“ Lösungen

Es wurden folgende Lösungen implementiert, die dem Schutz des Rechts auf Privatsphäre förderlich sind (siehe Leitlinien, Abschnitt 3.4):

- niedrigauflösende Kameras
- Einzelbildtechnologie (picture-by-picture technology)

3. ÜBERWACHTE BEREICHE

Die Kameras befinden sich an den Eingängen und Ausgängen der Gebäude, im Computerraum und im Fitnessraum.

Ansonsten wurden inner- oder außerhalb des Gebäudes keine weiteren Kameras installiert. Mit Ausnahme des Fitnessraums[1] werden keine Bereiche überwacht, in denen verstärkte Erwartungen an den Schutz der Privatsphäre gestellt werden, etwa Einzelbüros, Freizeitbereiche, Toilettenräume und andere (siehe Leitlinien, Abschnitt 6.8). Die Standorte der Kameras wurden gewissenhaft geprüft, um die Überwachung derjenigen Bereiche, die für die Verwendungszwecke nicht von Belang sind, auf ein Mindestmaß zu reduzieren (Leitlinien, Abschnitt 6.1).

Eine Überwachung außerhalb der Gebäude des EuHR im Hoheitsgebiet Luxemburgs findet gemäß den Empfehlungen in Abschnitt 6.5 der Leitlinien nicht statt.

---

[1] Die Installation einer Kamera im Fitnessraum erfolgte, um feststellen zu können, ob eine Person, die sich allein in dem Raum aufhält, einen Unfall erlitten hat oder erkrankt ist.

4. ERHEBUNG PERSONENBEZOGENER DATEN UND ZWECK

Das Videoüberwachungssystem ist ein konventionelles statisches System. Es zeichnet Einzelbilder digital auf. Es zeichnet die von den Kameras in dem überwachten Bereich gemachten Bilder zusammen mit Uhrzeit, Datum und Ort auf. Alle Kameras sind 24 Stunden am Tag und sieben Tage die Woche in Betrieb. In einigen Fällen ist es aufgrund der Bildqualität möglich, die Personen zu identifizieren, die sich im Erfassungsbereich der Kamera befinden (siehe Leitlinien, Abschnitt 6.4). Es wird keine Hightech- oder intelligente Videoüberwachungstechnologie eingesetzt (siehe Abschnitt 6.9 der Leitlinien), das System ist nicht mit anderen Systemen zusammengeschaltet (Abschnitt 6.10) und es werden keine verdeckte Überwachung (Abschnitt 6.11), Tonaufzeichnungen oder „talking CCTV“ (Abschnitt 6.12) verwendet.

Der EuRH setzt sein Videoüberwachungssystem einzig und allein zu Sicherheitszwecken und zum Zweck der Zugangskontrolle ein.

Das System wird weder zu anderen Zwecken noch zur Ermittlung verwendet (mit Ausnahme von Untersuchungen physischer Sicherheitsvorfälle wie Diebstähle oder unbefugter Zutritt). Nur in Ausnahmefällen können die Bilder im Rahmen eines förmlichen Disziplinarverfahrens oder eines strafrechtlichen Ermittlungsverfahrens (siehe Abschnitte 5.7, 5.8 und 10.3 der Leitlinien) an Ermittlungsbehörden übermittelt werden).

Der EuRH plant derzeit keine Ad-hoc-Überwachung (siehe Leitlinien, Abschnitt 3.5).

Es werden keine Webcams zur Videoüberwachung eingesetzt (siehe Abschnitt 5.10 der Leitlinien).

Es werden keine besonderen Datenkategorien erhoben (Abschnitt 6.7 der Leitlinien).

5. DATENZUGRIFF UND -WEITERGABE

5.1. Internes Sicherheitspersonal

Bildaufnahmen sind ausschließlich dem internen Sicherheitspersonal zugänglich.

5.2. Schulungen in datenschutzrechtlichen Fragen

Alle Mitarbeiter, die Zugriffsrechte auf die im Zuge der Videoüberwachung aufgezeichneten Bilder besitzen, wurden in datenschutzrechtlichen Fragen geschult.

5.3. Übermittlung und Weitergabe

Jede Übermittlung und Weitergabe von Daten außerhalb der Sicherheitsabteilung wird dokumentiert und setzt eine gründliche Prüfung der Notwendigkeit einer solchen Übermittlung sowie der Vereinbarkeit der Zwecke der Übermittlung mit dem ursprünglichen Ziel der Verarbeitung zu Sicherheits- und Zugangskontrollzwecken voraus (siehe Abschnitt 10 der Leitlinien). Das Register der Aufbewahrung und Übermittlung von Daten ist in Anlage 6 beigefügt (siehe Abschnitt 10.5 und 7.2 der Leitlinien). Bis zum 28. Oktober 2011 enthielt das

Register keine Einträge. Der behördliche Datenschutzbeauftragte (DSB) wird in jedem einzelnen Fall hinzugezogen. Der Leitung oder dem Direktorat für Personalangelegenheiten wird kein Zugriff gewährt.

5.4. Wie werden Informationen geschützt und gesichert?

Zum Schutz der Sicherheit des Videoüberwachungssystems, einschließlich der personenbezogenen Daten, wurde eine Reihe von technischen und organisatorischen Maßnahmen ergriffen.

6. WIE LANGE WERDEN DATEN AUFBEWAHRT?

Die Bilder werden höchstens 16 Tage lang (7 Tage im Gebäude K8) aufbewahrt. Anschließend werden alle Bilder durch neu aufgezeichnete Bilder physisch überschrieben. Wenn Bilder für weitere Untersuchungen oder als Beweismittel bei Sicherheitsvorfällen gespeichert werden müssen, können sie so lange aufbewahrt werden, wie dies notwendig ist. Ihre Aufbewahrung ist genau zu dokumentieren und die Notwendigkeit der Aufbewahrung muss regelmäßig überprüft werden. Jede Aufbewahrung von Bildern ist dem DSB anzuzeigen, der das Register der Aufbewahrung und Übermittlung von Daten führt (siehe Abschnitt 7 der Leitlinien.)

7. INFORMATION DER ÖFFENTLICHKEIT

7.1. Spezifische individuelle Hinweise

Personen müssen auch individuell darauf aufmerksam gemacht werden, dass sie von einer Kamera identifiziert wurden (etwa vom Sicherheitspersonal bei einer Sicherheitsuntersuchung), sofern eine oder mehrere der nachstehenden Bedingungen erfüllt sind:

die Identität der Person wird in Dateien bzw. Unterlagen festgehalten,

die Videoaufnahme wird gegen die Person verwendet,

die Videoaufnahme wird über die vorschriftsmäßige Aufbewahrungszeit hinaus gespeichert,

die Videoaufnahme wird an Empfänger außerhalb der Sicherheitsabteilung übermittelt *oder*

die Identität der Person wird jemandem außerhalb der Sicherheitsabteilung offengelegt.

Der behördliche Datenschutzbeauftragte des Organs wird in derartigen Fällen hinzugezogen, um zu gewährleisten, dass die Rechte der Person gewahrt werden.

8. ÜBERPRÜFUNG, BERICHTIGUNG UND LÖSCHUNG VON DATEN

Die Öffentlichkeit hat das Recht auf Zugang zu den vom EuRH gehaltenen, sie betreffenden Daten. Anträge auf Zugriff oder Berichtigung, Sperrung und/oder Löschung personenbezogener Daten sind an den Beauftragter für physische Sicherheit (ECA-Security@eca.europa.eu; Tel.: +352 4398 45911) zu richten. Es kann auch Kontakt zum behördlichen Datenschutzbeauftragten aufgenommen werden, wenn es um andere Fragen zur Verarbeitung personenbezogener Daten geht.

9. RECHT, SICH AN DEN EUROPÄISCHEN DATENSCHUTZBEAUFTRAGTEN ZU WENDEN

Jede Person hat das Recht, sich an den Europäischen Datenschutzbeauftragten (edps@edps.europa.eu) zu wenden, wenn sie der Auffassung ist, dass ihre Rechte aus der Verordnung Nr. 45/2001 aufgrund der Verarbeitung der sie betreffenden personenbezogenen Daten durch den EuRH verletzt wurden. Vorher empfiehlt der EuRH den Betroffenen jedoch, sich hierfür zunächst zu wenden an:

- den Sicherheitsbeauftragten (Kontaktangaben siehe oben) und/oder
- den behördlichen Datenschutzbeauftragten (ECA-Data-Protection@eca.europa.eu; Tel.: +352 4398 47777)

10. RECHTSQUELLEN

Verordnung Nr. 45/2001

Videoüberwachung - Leitlinien des EDSB