Generaldirektion Infrastrukturen

Videoüberwachungsstrategie

Gerichtshof der Europäischen Union

INHALTSVERZEICHNIS

1. Ziel und Umfang der Videoüberwachungsstrategie des Organs

Am 5. Juli 2005 hat der „Gebäude"-Ausschuss des Gerichtshofs der Europäischen Union das *Konzept zur umfassenden Sicherung des Gebäudekomplexes des Gerichtshofs der Europäischen Union* zur Kenntnis genommen.

Zu den verschiedenen Empfehlungen dieser Studie gehörte die Installation eines Videoüberwachungssystems, um die Sicherheit von Gebäuden, Vermögenswerten und Personen zu gewährleisten.

Das Organ hat daher ein Videoüberwachungssystem eingerichtet. Ein Bericht über den gegenwärtigen Betrieb dieses Systems wurde dem Verwaltungsausschuss vorlegt und von diesem in seiner Sitzung vom 1. Juli 2009 zur Kenntnis genommen.

Das vorliegende Dokument beschreibt das aktuelle Videoüberwachungssystem und die Maßnahmen, die das Organ zum Schutz der personenbezogenen Daten, der Privatsphäre und anderer Grundrechte ergriffen hat.

2. Schutz der Privatsphäre, Datenschutz und Konformität des Videoüberwachungssystems

2.1 Überprüfung des bestehenden Systems

Bereits vor Herausgabe der Leitlinien des Europäischen Datenschutzbeauftragten (im Folgenden: EDSB) zur Videoüberwachung vom 17. März 2010 (im Folgenden: Leitlinien) hat der Gerichtshof der Europäischen Union ein Videoüberwachungssystem betrieben.

Dieses System und die Verfahren des Organs sind mit den Rechtsvorschriften über den Schutz personenbezogener Daten und insbesondere mit den Empfehlungen des EDSB in den Leitlinien[1] in Einklang gebracht worden.

2.2 Compliance-Status

Der Gerichtshof der Europäischen Union verarbeitet Bilder im Einklang mit der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (im Folgenden: Verordnung Nr. 45/2001) und den Leitlinien.

[1] Die Leitlinien zur Videoüberwachung sind auf der Website des EDSB verfügbar:

https://secure.edps.europa.eu/EDPSWEB/edps/lang/de/Supervision/Guidelines

2.3 Internes Audit

Alle zwei Jahre wird ein internes Audit durchgeführt.

2.4 Mitteilung des Compliance-Status an den EDSB

Die mit dem Videoüberwachungssystem verbundene Verarbeitung personenbezogener Daten wurde dem EDSB erstmals im April 2009 mitgeteilt.
Im Anschluss an die Annahme der vorliegenden Videoüberwachungsstrategie hat der Gerichtshof der Europäischen Union dem EDSB durch Übermittlung eines Exemplars des vorliegenden Dokuments den Compliance-Status mitgeteilt.

2.5 Kontakt zur zuständigen Datenschutzbehörde des Mitgliedstaats

Die zuständige Datenschutzbehörde in Luxemburg (Commission nationale pour la protection des données – CNPD) wurde im November 2006 unterrichtet. Ihre Bemerkungen und Empfehlungen[2] wurden berücksichtigt.

2.6 Transparenz

Die Videoüberwachungsstrategie ist einsehbar:
- auf der Intranetseite des Sicherheitsdienstes: http://intranet/infrastructures/indispensables/securite.htm
- auf der Intranetseite des Datenschutzbeauftragten: http://intranet/dpo/FR/Home_FR.htm
- auf der Website des Gerichtshofs der Europäischen Union:
- http://curia.europa.eu/jcms/jcms/P_127468: Das Organ > Zugang zum Gerichtshof > Allgemeine Bedingungen.

2.7 Regelmäßige Überprüfungen

Der Sicherheitsdienst des Organs führt alle zwei Jahre eine Datenschutzprüfung durch. Dabei wird geprüft, ob
- ein Videoüberwachungssystem nach wie vor notwendig ist,
- das System mit den erklärten Zielen im Einklang steht,
- keine angemessenen Alternativen bestehen.

Bei diesen regelmäßigen Überprüfungen wird auch geprüft, ob die Videoüberwachungsstrategie des Gerichtshofs der Europäischen Union nach wie vor mit der Verordnung Nr. 45/2001 und den Leitlinien übereinstimmt (Angemessenheitsaudit) und ob sie in der Praxis eingehalten wird (Konformitätsaudit).

[2] Speziell in einem Schreiben an den für die Verarbeitung Verantwortlichen vom 15.3.2014 hat die CNPD ausgeführt, dass *„allein die Verordnung Nr. 45/2001 Anwendung findet, da das Videoüberwachungssystem … sich strikt auf den privaten Bereich beschränkt und jede Überwachung des öffentlichen Bereichs ausgeschlossen ist“*.

2.8 „Privatsphärenfreundliche“ technische Lösungen

Der Gerichtshof der Europäischen Union hat technische Lösungen implementiert, die dem Schutz des Rechts auf Privatsphäre förderlich sind:

- Die Bildwinkel und die Objektive der Kameras wurden so gewählt, dass nur die zu überwachenden Bereiche erfasst werden;
- die Gebäudebereiche, bei denen noch höhere Erwartungen an den Schutz der Privatsphäre gestellt werden, werden nicht mit Kameras überwacht;
- Zugang zu den aufgezeichneten Bildern ist für autorisierte Personen, d. h. eine kleine Zahl von Mitarbeitern des Sicherheitsdienstes, nur mit einer speziellen Software, einem Nutzerprofil und einem Passwort möglich;
- sämtliche Manipulationen am System werden aufgezeichnet (Registrierung der Handlung und des Nutzers, der sie vorgenommen hat).

3. Überwachte Bereiche

Dem Sicherheitskonzept entsprechend wurde am derzeitigen Standort (mit einer Fläche von etwa 220 000 m²) ein Videoüberwachungssystem mit 526 Kameras installiert.

Dieses System erfasst:

- Außenbereiche / Notausgänge
  Ziel: Verhinderung von Einbrüchen und asozialem Verhalten

- Zugang zu den Empfangsbereichen
  Ziel: Überwachung der Ein- und Ausgangsbewegungen

- Zugang zu den Tiefgaragen (Schranken und Tore) / Rampen und Verkehrswege auf den unterschiedlichen Ebenen der Tiefgaragen
  Ziel: Verhinderung von Schäden an Vermögenswerten des Organs und Angriffen auf Personen, Unterstützung bei der Schlichtung von entsprechenden Streitigkeiten

- Laderampen und Lagerräume
  Ziel: Überwachung der Anlieferungen und des Zugangs zu den Laderampen und Lagerräumen, Schutz sensibler technischer Anlagen

- öffentliche Bereiche in den Gebäuden
  Ziel: Beobachtung der allgemeinen Lage durch die Sicherheitszentrale, um gegebenenfalls eingreifen zu können (Störungen der Ordnung, zurückgelassener verdächtiger Gegenstand, Sturz einer Person usw.); Überwachung der Kunstwerke, schnelles Eingreifen bei Brand oder Unwohlsein.

- Übergänge in die geschützten privaten Bereiche
  Ziel: Verhinderung des unbefugten Eindringens in diese Bereiche und Leistung – in Kombination mit der Gegensprechanlage – der für die Nutzer notwendigen

Unterstützung bei Schwierigkeiten mit den Zugangskontrollanlagen (Kontrollschleusen und Ausweislesegeräte).

Karten mit den Standorten der Kameras sind beim Sicherheitsdienst des Organs verfügbar und dort einsehbar. Auf Anfrage können diese Karten vom für die Datenverarbeitung Verantwortlichen, vom Datenschutzbeauftragten des Organs (im Folgenden: DSB) und vom EDSB eingesehen werden.

Auf Bereiche, bei denen höhere Erwartungen an den Schutz der Privatsphäre gestellt werden, sind keine Kameras gerichtet.

4. Erhobene personenbezogene Daten und Zweck der Erhebung

4.1 Kurzbeschreibung und ausführliche technische Spezifikationen des Systems

Das Videoüberwachungssystem nimmt digitale Bilder auf und ist mit Bewegungsmeldern ausgestattet. Es erfasst die von den Kameras in den überwachten Bereichen festgestellten Bewegungen sowie das Datum, die Uhrzeit und den Ort. Die Kameras sind 24 Stunden am Tag und sieben Tage die Woche in Betrieb. Die Bildqualität kann je nach Standort eine Identifizierung von Personen ermöglichen. Die Mehrzahl der Kameras ist fest montiert. Einzelne Kameras verfügen über beschränkte optische Zoom-Fähigkeiten, die es ermöglichen, einen Ort oder im Bedarfsfall eine Person heranzuzoomen, um ihr zu folgen.

Das Videoüberwachungssystem setzt keine „intelligenten“ Technologien ein, ist nicht mit anderen Systemen zusammengeschaltet, setzt keine verdeckte Überwachung ein, zeichnet keinen Ton auf und setzt keine „talking CCTV“ ein.

4.2 Zweck der Überwachung

Das Organ setzt sein Videoüberwachungssystem ausschließlich zu Zwecken der Zugangskontrolle und der Sicherheit ein (Sicherheit von Personen, Gebäuden und Informationen).
Diese Anlagen ergänzen die Systeme der Zugangskontrolle, der Notausgangssicherung und des Brandschutzes.
Das Videoüberwachungssystem ist Teil der Maßnahmen zur Förderung der allgemeinen Sicherheitsstrategie und trägt zur Verhütung, Abschreckung und gegebenenfalls Untersuchung unbefugten Zutritts bei (gefährdete Räume, IT-Infrastrukturen und operative Informationen).
Darüber hinaus hilft die Videoüberwachung bei der Verhütung, Erkennung und Untersuchung von Diebstählen von Ausrüstungs- oder Vermögensgegenständen, die sich im Besitz des Organs, seiner Mitarbeiter oder von Besuchern befinden. Sie trägt auch dazu bei, die Sicherheit der Gebäudenutzer zu gewährleisten (z. B. bei einem Brand oder tätlichen Übergriff).

4.3 Eingrenzung der Zweckbestimmung

Die Videoüberwachung wird nur zu den oben genannten Zwecken eingesetzt. Das Videoüberwachungssystem wird nicht zur Beurteilung der Leistung von Mitarbeitern oder zur Anwesenheitskontrolle eingesetzt.
Zur Ermittlung wird es nur bei einem Sicherheitsvorfall eingesetzt (Diebstahl, unbefugter Zutritt usw.). In Ausnahmefällen können die Bilder anderen amtlichen Stellen im Rahmen der Wahrnehmung ihrer Befugnisse und Zuständigkeiten (Ermittlungsverfahren, Disziplinarverfahren, OLAF usw.) übermittelt werden. Diese Übermittlung ist in Nr. *6.5 Übermittlung und Weitergabe* beschrieben.

4.4 Verdeckte Überwachung

Im Rahmen des Videoüberwachungssystems ist keine verdeckte Überwachung vorgesehen. In seltenen Fällen kann das Organ jedoch – ohne eine Verbindung zum allgemeinen Videoüberwachungssystem – Geräte zur verdeckten Überwachung einsetzen.

Der Einsatz dieser Geräte kann nur unter folgenden Bedingungen erfolgen:
- zur Suche nach Personen, die sich wiederholt unbefugt Zutritt verschafft, Diebstähle oder sonstige schwere Verstöße gegen Sicherheitsvorschriften begangen haben,
- für einen eng begrenzten Zeitraum,
- an genau bestimmten Standorten,
- auf der Grundlage einer dem Datenschutzbeauftragten des Organs zur Stellungnahme vorgelegten Folgenabschätzung,
- und auf Beschluss des Kanzlers des Gerichtshofs der Europäischen Union.

Die Geräte zur verdeckten Überwachung werden nur für die Dauer der Verstöße, die zu ihrem Einsatz geführt haben, eingesetzt. Sobald der oder die Täter identifiziert sind, werden die Geräte entfernt.

Der Standort der Geräte zur verdeckten Überwachung richtet sich nach dem Ort, an dem die Verstöße, die zu ihrem Einsatz geführt haben, begangen werden. Die Geräte können nicht in Räumen angebracht werden, in denen der Schutz der Intimsphäre selbstverständlich erwartet wird (Toiletten).

Der Einsatz verdeckter Kameras erfolgt unter strengen Bedingungen, die dem EDSB zur Vorabkontrolle mitgeteilt werden und sicherstellen, dass der Eingriff in die Privatsphäre minimiert wird.

4.5 Webcams

Mit dem Videoüberwachungssystem des Gerichtshofs der Europäischen Union sind keine Webcams verbunden.

4.6 Erhebung besonderer Datenkategorien

Es werden keine Daten der in Art. 10 der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz personenbezogener Daten[3] genannten besonderen Datenkategorien erhoben.

Bei Demonstrationen vor den Gebäuden des Gerichtshofs der Europäischen Union gelten folgende zusätzliche Garantien:

- Die Überwachung von Demonstrationen erfolgt nur aus Sicherheitsgründen;
- die Kameras können nicht auf die Gesichter von Personen gerichtet werden, und es wird nicht versucht, mit Hilfe der Kameras Personen zu erkennen, es sei denn, die öffentliche Sicherheit ist unmittelbar bedroht oder es handelt sich um gewalttätiges strafbares Verhalten (Vandalismus, tätliche Übergriffe);
- die Bilder werden nicht für die gezielte Datensuche (Data Mining) verwendet[3];
- alle Personen, die Videogeräte bedienen, werden geschult (vgl. Nr. *6.3 Schulungen in datenschutzrechtlichen Fragen*), um jede unverhältnismäßige Auswirkung auf die Privatsphäre und andere Grundrechte der aufgenommenen Teilnehmer einschließlich ihrer Versammlungsfreiheit zu vermeiden.

5. Legitimation und Rechtsgrundlage des Videoüberwachungssystems

Der Einsatz des Videoüberwachungssystems zu Zwecken der Sicherheit und der Zugangskontrolle ist erforderlich, um den reibungslosen Betrieb des Organs und die legitime Ausübung der ihm übertragenen öffentlichen Gewalt zu gewährleisten.

Der Betrieb des Videoüberwachungssystems, wie er beim Gerichtshof der Europäischen Union erfolgt, entspricht Art. 5 Buchst. a der Verordnung Nr. 45/2001.

Die vorliegende Videoüberwachungsstrategie, die Teil der Sicherheitsstrategien des Organs im weiteren Sinne ist, bietet eine ausführlichere und konkretere Rechtsgrundlage für die Videoüberwachung.

6. Zugang zu den Informationen und erhobenen Daten

6.1 Sicherheitsdienst des Organs und Wachdienst

Mit der Sichtung der in Echtzeit übertragenen Bilder sind Sicherheitsbedienstete eines Wachdienstes beauftragt[4].

[3] Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Daten über Gesundheit oder Sexualleben.

[4] Dieser Wachdienst ist ein Auftragsverarbeiter im Sinne von Art. 2 Buchst. e der Verordnung Nr. 45/2001. Er verarbeitet die personenbezogenen Daten unter den in Art. 23 dieser Verordnung vorgesehenen Bedingungen.

Die Sicherheitsbediensteten des Wachdienstes haben keinen Zugriff auf die aufgezeichneten Bilder.

Die Verdingungsunterlagen, die dem mit dem Wachdienst geschlossenen Dienstleistungsvertrag beigefügt sind, enthalten eine Vertraulichkeitsklausel und eine Bestimmung über den Datenschutz, um sicherzustellen, dass die Sicherheitsbediensteten den Schutz personenbezogener Informationen achten. In den Verdingungsunterlagen wird auch speziell auf die Videoüberwachung Bezug genommen (vgl. Anlagen 1a und 1b).

Nur die Mitarbeiter des Sicherheitsdienstes des Organs haben Zugriff auf die aufgezeichneten Bilder.
Alle Mitglieder des Sicherheitsdienstes müssen in Bezug auf den Einsatz des Videoüberwachungssystems eine Vertraulichkeitserklärung unterzeichnen.

6.2 Zugangsrechte

Im „Internen Videoüberwachungsverfahren“[5] ist klar ausgeführt, wer, unter welchen Bedingungen und in welchem Umfang Zugang zu den aufgezeichneten Bildern und den technischen Anlagen des Videoüberwachungssystems hat.

Ein Zugriff auf die aufgezeichneten Bilder ist nur mit einer speziellen Software, einem Nutzerprofil und einem Passwort möglich. Diese spezielle Software ist nur auf den Computern bestimmter Mitarbeiter des Sicherheitsdienstes des Organs installiert.

6.3 Schulungen in datenschutzrechtlichen Fragen

Alle Mitarbeiter mit Zugangsrechten, einschließlich der Sicherheitsbediensteten des Wachdienstes, wurden in datenschutzrechtlichen Fragen geschult.
Neue Mitglieder des Sicherheitspersonals erhalten bei Dienstantritt systematisch eine Schulung.
Alle zwei Jahre finden für die Mitarbeiter mit Zugangsrechten Workshops zu Themen in Verbindung mit der Einhaltung der Datenschutzvorschriften statt.

6.4 Verpflichtung des Sicherheitspersonals zu Vertraulichkeit

Jeder Mitarbeiter des Sicherheitsdienstes des Organs, der zur Bildverarbeitung berechtigt ist, hat nach seiner datenschutzrechtlichen Schulung eine Vertraulichkeitserklärung unterzeichnet.
Jeder Bedienstete des Wachdienstes, der zur Bildverarbeitung berechtigt ist, hat nach seiner datenschutzrechtlichen Schulung eine Vertraulichkeitserklärung unterzeichnet.

[5] Das Interne Videoüberwachungsverfahren ist ein internes Dokument, in dem festgelegt ist, wer berechtigt ist, die Bilder in Echtzeit anzusehen, die aufgezeichneten Bilder anzusehen, die Bilder zu kopieren, herunterzuladen, zu löschen und zu verarbeiten.

6.5 Übermittlung und Weitergabe

Eine Übermittlung oder Weitergabe von Daten kann nur durch den für die Datenverarbeitung Verantwortlichen, d. h. den Leiter des Sicherheitsdienstes, nach Anhörung des DSB erfolgen. Jede Übermittlung oder Weitergabe von Daten an Empfänger außerhalb des Sicherheitsdienstes setzt eine gründliche Prüfung ihrer Notwendigkeit sowie der Vereinbarkeit ihrer Zwecke mit den ursprünglich verfolgten Zielen, nämlich der Sicherheit und der Zugangskontrolle, voraus.

Die Übermittlungen werden systematisch in das Register der Aufbewahrung und Übermittlung von Daten eingetragen, das vom Leiter des Sicherheitsdienstes geführt wird.

Die Direktion für Humanressourcen und Personalverwaltung ist nicht berechtigt, auf die verarbeiteten Daten zuzugreifen.

Unter den in Art. 8 der Verordnung Nr. 45/2001 festgelegten Bedingungen können die Bilder der luxemburgischen Polizei übermittelt werden, wenn sich dies als für eine in Ausübung ihrer Zuständigkeiten geführte Untersuchung erforderlich erweist. Im Zweifelsfall zieht der Sicherheitsdienst den Rechtsberater für Verwaltungsangelegenheiten hinzu.

Bilder können in Ausnahmefällen auch übermittelt werden an

- den Gerichtshof, das Gericht und/oder das Gericht für den öffentlichen Dienst (GÖD) oder einen nationalen Richter sowie die Anwälte oder Bevollmächtigten einer Partei im Fall eines Rechtsstreits;
- die mit der Prüfung von Beschwerden beauftragte Stelle des Gerichtshofs, des Gerichts oder des GÖD, den Präsidenten und den Kanzler des betreffenden Gerichts sowie den Rechtsberater für Verwaltungsangelegenheiten im Fall einer gemäß Art. 90 Abs. 2 des Beamtenstatuts eingelegten Beschwerde;
- das OLAF im Fall einer nach der Verordnung Nr. 883/2013 und dem Beschluss des Gerichtshofs vom 12. Juli 2011 über die Bedingungen und Modalitäten der internen Untersuchungen zur Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen zum Nachteil der Interessen der Europäischen Union durchgeführten Untersuchung;
- die Personen, die auf einen Sicherheitsvorfall hin im Rahmen einer von der Anstellungsbehörde oder der zum Abschluss von Dienstverträgen ermächtigten Behörde angeordneten Verwaltungsuntersuchung oder im Rahmen eines nach den Vorschriften des Anhangs IX des Statuts der Beamten der EU eröffneten Disziplinarverfahrens tätig werden;
- den Präsidenten und den Kanzler des Gerichtshofs sowie die Beamten, die sie im Rahmen der ihnen durch Art. 20 Abs. 4 der Verfahrensordnung des Gerichtshofs übertragenen Aufgaben unterstützen;
- den EDSB gemäß Art. 47 Abs. 2 der Verordnung Nr. 45/2001;
- den DSB des Organs gemäß Nr. 4 des Anhangs der Verordnung Nr. 45/2001;
- den Europäischen Bürgerbeauftragten, soweit dies für die Bearbeitung einer bei ihm eingereichten Beschwerde erforderlich ist (Art. 228 AEUV).

7. Maßnahmen zum Schutz von Daten und Informationen

Die wichtigsten technischen und organisatorischen Maßnahmen, die zum Schutz der Sicherheit des Videoüberwachungssystems, einschließlich der personenbezogenen Daten, ergriffen wurden, sind:

- Die Server, auf denen die Bilder aufgezeichnet werden, befinden sich in gesicherten Räumen, die durch physische Sicherheitsmaßnahmen geschützt sind; die IT-Anlagen sind durch Firewalls geschützt;
- jedes Mitglied des Sicherheitspersonals (intern und extern) hat eine Vertraulichkeitserklärung unterzeichnet;
- die Zugangsrechte der Nutzer des Videoüberwachungssystems sind auf die Tools beschränkt, die für die Ausübung ihrer Aufgaben erforderlich sind;
- nur der vom für die Verarbeitung Verantwortlichen benannte Systemadministrator ist berechtigt, Nutzern Zugangsrechte zu gewähren, diese abzuändern oder aufzuheben. Die Gewährung, Änderung oder Aufhebung von Zugangsrechten erfolgt gemäß den im Internen Videoüberwachungsverfahren festgelegten Kriterien;
- das Interne Videoüberwachungsverfahren umfasst eine aktualisierte Liste aller zugangsberechtigten Personen, in der der Umfang ihrer Zugangsrechte festgelegt ist.

8. Aufbewahrung der Daten

Die Bilder werden höchstens 30 Tage lang aufbewahrt.
Anschließend werden alle Aufzeichnungen automatisch gelöscht.
Die Wahl dieses Zeitraums ist begründet durch

- gegenwärtige Erfahrungen, dass Sicherheitsvorfälle dem Sicherheitsdienst des Organs häufig erst nach über zwei Wochen angezeigt werden;
- die Praxis von Tätern/Terroristen, vor Begehung einer rechtswidrigen Handlung die Gebäude auszukundschaften;
- die große Zahl der Besucher (ungefähr 100 000 Personen jährlich).

Bestimmte Bilder können länger aufbewahrt werden, wenn sie für weitere Untersuchungen oder als Beweismittel bei einem Sicherheitsvorfall erforderlich sind. Diese Aufbewahrung wird dokumentiert (elektronisches Register), und die Gründe, aus denen die Bilder länger als 30 Tage lang aufbewahrt werden, werden angegeben. Eine Papierkopie des Registers der Aufbewahrung und Übermittlung ist als Anlage 2a und 2b beigefügt. Die Notwendigkeit dieser Aufbewahrung wird regelmäßig überprüft.

Die Videoüberwachung wird von den Sicherheitsbediensteten in der Sicherheits- und Brandzentrale (PCS/PCI) 24 Stunden am Tag und sieben Tage die Woche in Echtzeit verfolgt.

9. Information der Öffentlichkeit und spezifische individuelle Information

9.1 Information über verschiedene Medien

Die Öffentlichkeit wird angemessen und umfassend über die Videoüberwachung informiert. Diese Unterrichtung erfolgt über folgende Medien:

- An den verschiedenen Eingängen der Gebäude sind Hinweistafeln angebracht. Diese Tafeln weisen auf das Videoüberwachungssystem hin und geben insbesondere die Dauer der Aufbewahrung der Bilder sowie die Kontaktdaten des zuständigen Dienstes an;
- ein Informationsblatt mit den nach Art. 12 der Verordnung Nr. 45/2001 vorgeschriebenen Informationen ist an den Empfängen der Gebäude, auf den Intranetseiten des Sicherheitsdienstes und des Datenschutzbeauftragten sowie auf der Website des Organs (http://curia.europa.eu/jcms/jcms/P_127468: Organ > Zugang zum Gerichtshof > Allgemeine Bedingungen) verfügbar. Dieses Blatt enthält eine Telefonnummer und eine E-Mail-Adresse, damit interessierte Personen weitere Auskünfte erhalten können;
- die vorliegende Videoüberwachungsstrategie ist auf den Intranetseiten des Sicherheitsdienstes und des Datenschutzbeauftragten sowie der Internetseite des Gerichtshofs der Europäischen Union einsehbar (vgl. *Nr. 2.6 Transparenz*).

Kopien der Hinweistafeln und des Informationsblatts sind in den Anlagen 3a und 3b beigefügt.

9.2 Spezifische individuelle Hinweise

Werden Personen auf den Bildern identifiziert (z. B. für eine Sicherheitsuntersuchung), müssen sie individuell darauf aufmerksam gemacht werden, wenn mindestens eine der nachstehenden Bedingungen erfüllt sind:

- Ihre Identität wird in einer Datei festgehalten;
- die Bildsequenz wird gegen die betreffende Person verwendet;
- die Bildsequenz wird über den vorgesehenen Zeitraum hinaus gespeichert;
- die Bildsequenz wird an einen Empfänger außerhalb des Sicherheitsdienstes übermittelt;
- die Identität der Person wird Personen außerhalb des Sicherheitsdienstes mitgeteilt.

Diese individuelle Unterrichtung kann gemäß Art. 20 Abs. 1 Buchst. a der Verordnung Nr. 45/2001 aufgeschoben werden, wenn dies für die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten notwendig ist. Wird die Anwendung dieser Einschränkung in Betracht gezogen, ist der DSB zu konsultieren.

10. Rechte der Betroffenen

Die gefilmten Personen haben das Recht auf Zugang zu den sie betreffenden personenbezogenen Daten und das Recht, diese berichtigen zu lassen, wenn sie falsch oder unvollständig sind.

Was die Wahrnehmung des Zugangsrechts angeht, so kann eine Betrachtung der Bilder organisiert werden, oder der Antragsteller kann eine Kopie der aufgezeichneten Bilder erhalten. In diesem Fall hat sich der Antragsteller vor der Betrachtung der Bilder auszuweisen. Er muss außerdem Datum, Uhrzeit, Ort und die Umstände der Aufzeichnung angeben.

Gegenwärtig können die Antragsteller die Bilder kostenfrei betrachten und, wenn ein legitimes Interesse geltend gemacht wird, unentgeltlich eine Kopie erhalten. Der Grundsatz der Unentgeltlichkeit kann überprüft werden, falls die Zahl der Anträge erheblich steigen sollte.

Unter den in den Art. 15 und 16 der Verordnung Nr. 45/2001 genannten Voraussetzungen können die betroffenen Personen auch die Sperrung oder Löschung der sie betreffenden personenbezogenen Daten verlangen. Im Fall eines Löschungsantrags konsultiert der für die Verarbeitung Verantwortliche den DSB.

Die Rechte der betroffenen Personen können nach Art. 20 Abs. 1 Buchst. a der Verordnung Nr. 45/2001 eingeschränkt werden, wenn dies für die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten notwendig ist.

Die Rechte der betroffenen Personen können auch nach Art. 20 Abs. 1 Buchst. c der Verordnung Nr. 45/2001 eingeschränkt werden, wenn dies für den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen notwendig ist.
Wünscht eine betroffene Person z. B. Zugang zu Sequenzen, auf denen sie zu sehen ist, kann eine Einschränkung ihres Zugangsrechts erforderlich sein, wenn auf denselben Sequenzen auch eine andere Person zu sehen ist, deren Einwilligung nicht eingeholt werden kann, da das gegenwärtig verwendete Videoüberwachungssystem es nicht ermöglicht, das Bild einer Person zu verdecken.

Der für die Verarbeitung Verantwortliche konsultiert den DSB, wenn eine Einschränkung der Rechte der betroffenen Personen in Betracht gezogen wird.

Anträge auf Zugang, Berichtigung, Sperrung oder Löschung sind an folgende Person zu richten:

Leiter des Sicherheitsdienstes, Für die Verarbeitung Verantwortlicher
Gerichtshof der Europäischen Union
L-2925 Luxemburg
Tel.: +352 4303-1
securite@curia.europa.eu

Der Sicherheitsdienst kann auch bei anderen Fragen zur Verarbeitung personenbezogener Daten betreffend das vom Gerichtshof installierte Videoüberwachungssystem kontaktiert werden.

Der Sicherheitsdienst beantwortet jeden Antrag nach Möglichkeit innerhalb von 15 Werktagen. Kann diese Frist nicht eingehalten werden, wird der Antragsteller innerhalb dieser 15 Tage über den Stand der Bearbeitung seines Antrags und die Gründe unterrichtet, aus denen er nicht innerhalb der vorgesehenen Frist bearbeitet werden konnte. In jedem Fall muss spätestens nach drei Monaten eine Antwort erteilt werden.

11. Rechtsbehelfsbelehrung

Gemäß Art. 32 Abs. 2 der Verordnung Nr. 45/2001 kann jede betroffene Person, unbeschadet der Einlegung eines Rechtsbehelfs bei Gericht, beim EDSB (edps@edps.europa.eu) eine Beschwerde einreichen, wenn sie der Ansicht ist, dass die ihr in Art. 16 des Vertrags über die Arbeitsweise der Europäischen Union eingeräumten Rechte infolge der Verarbeitung von personenbezogenen Daten durch das Organ verletzt wurden.

Den betroffenen Personen wird empfohlen, sich vor der Einlegung einer Beschwerde mit ihrem Anliegen an folgende Personen zu wenden:

Leiter des Sicherheitsdienstes, Für die Verarbeitung Verantwortlicher
Gerichtshof der Europäischen Union
L-2925 Luxemburg
Tel.: +352 4303-1
securite@curia.europa.eu

und/oder

Datenschutzbeauftragter
Gerichtshof der Europäischen Union
L-2925 Luxemburg
Tel.: +352 4303-1
DataProtectionOfficer@curia.europa.eu

Mitarbeiter des Gerichtshofs können gemäß Art. 90 des Beamtenstatuts bei ihrer Anstellungsbehörde bzw. zum Abschluss von Dienstverträgen ermächtigten Behörde eine Überprüfung beantragen.

Anlagen

Anlage 1a *Auszug aus Art. 16 des Vertrags CJ 03/2010 über den Datenschutz*

Anlage 1b: *Auszug aus den Verdingungsunterlagen der Ausschreibung CJ 03/2010 über das Videoüberwachungssystem*

Anlage 2a: *Register der Aufbewahrung von Daten*

Anlage 2b: *Register der Übermittlung von Daten*

Anlage 3a: *Hinweistafeln*

Anlage 3b: *Informationsblatt*

Anhang 1a zur Videoüberwachungsstrategie

Artikel 16 - Datenschutz

1. Vom Gerichtshof der Europäischen Union verarbeitete Daten

   a. Der Gerichtshof der Europäischen Union verarbeitet personenbezogene Daten im Einklang mit der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr.

   b. Diese Daten werden ausschließlich für die Zwecke der Durchführung, der Verwaltung und Überwachung des Vertrags durch die Direktion Gebäude und die Direktion Haushalt und finanzielle Angelegenheiten verarbeitet, vorbehaltlich einer etwaigen Übermittlung dieser Daten an Einrichtungen, die nach dem Recht der Europäischen Union mit einer Kontroll- oder Inspektionsaufgabe betraut sind.

   c. Trifft auf den Auftragnehmer einer der in den Artikeln 93 und 94 der Haushaltsordnung (Verordnung Nr. 1605/2002 des Rates vom 25. Juni 2002) genannten Ausschlussgründe zu, werden die ihn betreffenden Daten in der in Artikel 95 dieser Verordnung vorgesehenen Datenbank gespeichert und können von der Kommission an Personen übermittelt werden, die von anderen Organen, Agenturen, Behörden und Einrichtungen im Sinne dieses Artikels gemäß Artikel 134a Absatz 2 der Verordnung Nr. 2342/2002 über die Modalitäten der Haushaltsordnung in geänderter Fassung und der Verordnung (EG,17 / 109 COUR DE JUSTICE DE L'UNION EUROPEENNE Appel d'offres CJ 03/2010 26 mars 2010 Euratom) Nr. 1302/2008 der Kommission vom 17. Dezember 2008 über die zentrale Ausschlussdatenbank zum Empfang dieser Daten berechtigt wurden.

   d. Im Rahmen der Vertragserfüllung können folgende Datenkategorien gespeichert werden:

- ➔ Name, Adresse, Telefon- und Telefaxnummer, E-Mail-Adresse;
- ➔ Daten, die im Pass oder im Staatsangehörigkeitsnachweis enthalten sind (Kopie);
- ➔ Nachweis der Stellung als Selbständiger, Nachweis des Steuerstatus;
- ➔ Bankverbindung (Kontonummer, Name der Bank, IBAN-Code);
- ➔ Daten, die in einem Auszug aus dem Strafregister, einer Bescheinigung über die (Nicht-)Entrichtung von Sozialversicherungsbeiträgen oder Steuern enthalten sind;
- ➔ Lebenslauf;
- ➔ Liste der wichtigsten Veröffentlichungen oder Werke;
- ➔ Erklärung über den Umsatz des Bieters;
- ➔ Erklärung von Banken oder Nachweis einer Berufshaftpflichtversicherung;

➔ andere Daten, die im Zusammenhang mit dem Auftragnehmer stehen und von diesem im Rahmen der Vertragserfüllung übermittelt wurden.

Darüber hinaus werden personenbezogene Daten von den an der Bewertung der Vertragsdurchführung Beteiligten erzeugt (insbesondere Bewertungsdaten).

e. Der Rechnungshof, der Fachausschuss für finanzielle Unregelmäßigkeiten, der interne Prüfer (im Rahmen der ihm durch die Artikel 85 bis 87 der Haushaltsordnung übertragenen Aufgaben), das Europäische Parlament (im Rahmen des Entlastungsverfahrens), das OLAF, der Überwachungsausschuss des OLAF (gemäß Artikel 11 der Verordnung Nr. 1073/1999), die Gerichte des Gerichtshofs der Europäischen Union, die zuständigen Gerichte (im Allgemeinen die luxemburgischen Gerichte) im Fall eines Rechtsstreits über die Durchführung des Auftrags, der Präsident und der Kanzler des Gerichtshofs sowie die Beamten, die sie im Rahmen der ihnen durch Artikel 20 Abs. 4 der Verfahrensordnung des Gerichtshofs übertragenen Aufgaben unterstützen, und der Rechtsberater für Verwaltungsangelegenheiten können im Rahmen ihrer jeweiligen Zuständigkeiten Empfänger sein.

f. Gemäß Artikel 49 der Verordnung Nr. 2342/2002 sind die Unterlagen über den Auftrag, die personenbezogene Daten enthalten, fünf Jahre lang aufzubewahren, gerechnet ab dem Zeitpunkt der Entlastung des Parlaments betreffend den Haushalt des Jahres, in dem die letzte Handlung zur Durchführung des Auftrags vorgenommen wurde oder die die im Rahmen des Auftrags zugunsten des Auftraggebers bestehende vertragliche oder gesetzliche Gewährleistung endet. Die in den Belegen enthaltenen personenbezogenen Daten werden nach Möglichkeit gelöscht, sofern sie nicht zur Haushaltsentlastung, zur Kontrolle und zur Prüfung benötigt werden.

g. Auf Antrag werden dem Auftragnehmer und Personen, von denen personenbezogene Daten im Rahmen der Ausführung dieses Vertrags verarbeitet werden, ihre personenbezogenen Daten mitgeteilt und unrichtige oder unvollständige Daten berichtigt. Die Betroffenen werden gebeten, sich mit allen Fragen zur Verarbeitung dieser Daten an den Leiter des Referats „Immobilien und Sicherheit“ zu wenden. Sie können auch jederzeit den Europäischen Datenschutzbeauftragten anrufen.

h. Der (die) Vertreter des Auftragnehmers ist (sind) verpflichtet, die Personen, auf die sich die im Rahmen dieses Vertrags verwendeten personenbezogenen Daten beziehen, über Art, Zwecke und Merkmale der Verarbeitung (Datenkategorien, Adressatenkategorien, Aufbewahrungsfrist usw.) und die vorstehend beschriebenen Rechte zu informieren.

2. <u>Für den Gerichtshof der Europäischen Union verarbeitete Daten</u>

a. Der Auftragnehmer handelt auf Weisung des für die Verarbeitung Verantwortlichen.

b. Er beachtet die Vorschriften über den Schutz personenbezogener Daten.

c. Bezüglich der Vertraulichkeit und der Sicherheit der Daten obliegen die in den Artikeln 21 und 22 der Verordnung (EG) Nr. 45/2001 genannten Verpflichtungen auch dem Auftragnehmer, es sei denn, er unterliegt aufgrund von Artikel 16 oder Artikel 17 Absatz 3 zweiter Gedankenstrich der Richtlinie 95/46/EG bereits Verpflichtungen in Bezug auf Vertraulichkeit und Sicherheit, die in den nationalen Rechtsvorschriften von einem der Mitgliedstaaten festgelegt sind.

7.2.3. System der Zugangskontrolle und der Einbruchssicherung

Der Gerichtshof stellt dem Dienstleistungserbringer ein zentralisiertes System zur Verfügung, das den gesamten Standort erfasst und es ermöglicht, die Zugänge zu kontrollieren und Einbruchsversuche zu erkennen. Es wird in Echtzeit über das Tool GSC betrieben. Bei eingeschränkter Betriebsfähigkeit kann der Wachhabende in der Sicherheitszentrale das native Teilsystem betreiben.
Das Besucherverwaltungsmodul wird von den Mitarbeitern an den Empfängen betrieben.

7.2.4. Videoüberwachungssystem

7.2.4.1. Allgemeines

Der Gerichtshof stellt dem Dienstleistungserbringer das vollständig digitale Zentralsystem mit folgenden Anlagen und Teilsystemen zur Verfügung:

➔ fest montierte und mobile Videoüberwachungskameras;

➔ digitale Aufzeichnungsgeräte mit großer Speicherkapazität und Funktion des Masterns, der automatischen kontinuierlichen Vor- und Nachalarmaufzeichnung und der Standbildaufzeichnung;

➔ Videodetektionssystem innen und außen (automatische Erkennung von Bewegungen im Sichtfeld der Kameras).

Die Überwachung der wichtigsten Zugangskontrollbarrieren und der sensiblen Bereiche wird durch fest montierte Kameras gewährleistet.

Die Überwachung der Außenbereiche der Gebäude wird durch fest montierte Kameras mit Videodetektion gewährleistet, die im Zweifelsfall durch mobile Kameras ergänzt werden.

Das Videoüberwachungssystem wird in Echtzeit mit dem Tool GSC betrieben. Bei eingeschränkter Betriebsfähigkeit kann der Wachhabende in der Sicherheitszentrale das native Teilsystem betreiben.

7.2.4.2. Schutz der Privatsphäre – Datenschutz

Der Dienstleistungserbringer handelt auf Weisung des für die Verarbeitung Verantwortlichen. Er beachtet die Vorschriften über den Schutz personenbezogener Daten, insbesondere

➔ die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, insbesondere die Bestimmungen über die Vertraulichkeit und die Sicherheit der Daten (Artikel 21 und 22 der Verordnung);

➔ die Leitlinien des Europäischen Datenschutzbeauftragten (ESDB) zur Videoüberwachung;

➔ die Videoüberwachungsstrategie des Gerichtshofs;

➔ die Vorgaben des Gerichtshofs;

➔ die Empfehlungen des Europäischen Datenschutzbeauftragten (ESDB) oder des Datenschutzbeauftragten des Gerichtshofs im Rahmen der Ausübung ihrer Kontroll-/Inspektions- oder Konsultationsaufgaben.

Der Dienstleistungserbringer verpflichtet sich, die Mitarbeiter, die die Kameras betreiben, angemessen zu schulen, insbesondere hinsichtlich der Datenschutzverpflichtungen und der Leitlinien des Europäischen Datenschutzbeauftragten (ESDB) zur Videoüberwachung.

Anhang 2a - REGISTER DER AUFBEWAHRUNG VON AUFZEICHNUNGEN (gemäß Nr. 7.2 der Leitlinien)

Nr.	Datum des Vorfalls	Uhrzeit		Kamera		Beschreibung des Vorfalls	Grund der Aufbewahrung	Voraussichtliches Datum der Überprüfung	Name der Aufzeichnung
		Beginn	Ende	Nummer	Standort				

Anhang 2b - REGISTER DER ÜBERMITTLUNG UND WEITERGABE (gemäß Nr. 10.5 der Leitlinien)

Nr.	Datum des Vorfalls	Kenndaten des Antragstellers				Person, die die Übermittlung genehmigt hat			Kurzbeschreibung des Inhalts der Aufzeichnungen	Begründung des Antrags und der Genehmigung der Übermittlung	Übermittlung	Gezeigt	Falls Informationen mündlich weitergegeben wurden, erläutern Sie, welcher Art diese sind
		Name	Vorname	Funktion	Dienst	Name	Vorname	Funktion					

Anhang 3a - Hinweistafeln

VIDÉOSURVEILLANCE

Pour votre sécurité, ce bâtiment et son voisinage immédiat sont placés sous vidéosurveillance.

Les images sont conservées pendant 30 jours.

Pour de plus amples informations, veuillez consulter la page http://curia.europa.eu/jcms/jcms/P_127468 ou prendre contact avec la section sécurité en téléphonant au +352 43031ou en adressant un courriel à securite@curia.europa.eu

VIDEOÜBERWACHUNG

Zu Ihrer Sicherheit werden dieses Gebäude und seine unmittelbare Umgebung videoüberwacht.

Die Aufnahmen werden 30 Tage lang gespeichert.

Weitere Auskünfte erhalten Sie unter der adresse http://curia.europa.eu/jcms/jcms/P_127468 Sie Können sich aber auch mit der Sicherheitsabteilung unter +352 43031 oder securite@curia.europa.eu in Verbindung setzen

VIDEO SURVEILLANCE

For your safety and security, this building and its immediate vicinty are under video-surveillance.

Recording are retained for 30 days.

For further information, please consult http://curia.europa.eu/jcms/jcms/P_127468 or contact the security section at +352 43031 or securite@curia.europa.eu

Anhang 3b - Informationsblatt

Informationsblatt zur Videoüberwachung in den Gebäuden des Gerichtshofs der Europäischen Union

Dieses Informationsblatt enthält Informationen über das vom Organ installierte allgemeine Videoüberwachungssystem (1) und zur Möglichkeit, eine Ad-hoc-Vorrichtung zu verwenden (2).

1. Informationen zur allgemeinen Videoüberwachung

Das Organ hat ein Videoüberwachungssystem installiert, um die allgemeine Sicherheit von Personen und Vermögensgegenständen gemäß dem Konzept zur Sicherung des Gebäudekomplexes des Gerichtshofs der Europäischen Union zu gewährleisten. Die Zwecke und Einzelheiten der Verarbeitung der gefilmten Bilder sind in dem Dokument „Videoüberwachungsstrategie“ beschrieben, das auf der Internetseite des Organs sowie auf den Intranetseiten des Sicherheitsdienstes und des Datenschutzbeauftragten einsehbar ist.

Überwachungskameras sind sowohl innerhalb als auch außerhalb der Gebäude des Organs angebracht (zufällige oder gesteuerte Auswahl der gefilmten Orte).

Die Bilder von den betroffenen Personen (Person, die Gebäude des Organs betritt oder sich in unmittelbarer Nähe der Gebäude befindet) sind die einzigen vom System gesammelten Daten.

Der für die Verarbeitung der Daten Verantwortliche ist der Leiter des Sicherheitsdienstes, Tel.: +352 4303-1, securite@curia.europa.eu.

Die Bilder werden aufgezeichnet und verwendet im Einklang mit

- der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr,
- den Empfehlungen des Europäischen Datenschutzbeauftragten (ESDB) in den Leitlinien zur Videoüberwachung vom 17. März 2010[1].

Die Bilder werden zu folgenden Zwecken verarbeitet:

- Zugangs- und Sicherheitskontrollen (Sicherheit von Personen, Gebäuden, Vermögensgegenständen und Informationen);

[1] Die Leitlinien zur Videoüberwachung sind auf der Internetseite des ESDB verfügbar: https://secure.edps.europa.eu/EDPSWEB/edps/lang/de/Supervision/Guidelines

- Lokalisierung eines Brandherds, Abschätzung der Folgen einer etwaigen Evakuierung eines Gebäudes, Überwachung der Notausgänge;
- Überwachung der Kunstwerke;
- Abschreckung (Beschädigung von Vermögensgegenständen des Organs, Angriffe auf Personen);
- Ermittlung der für Zuwiderhandlungen Verantwortlichen.

Die aufgezeichneten Bilder werden höchstens 30 Tage lang aufbewahrt. Bei Verdacht auf eine Zuwiderhandlung bzw. deren Feststellung werden die entsprechenden Daten jedoch für die Dauer der Untersuchung und des sich daraus gegebenenfalls ergebenden Verfahrens (z. B. eines Disziplinar- oder Strafverfahrens) aufbewahrt. Die aufgezeichneten Bilder sind nur einer begrenzten Zahl von Personen zugänglich, und alle technischen und physischen Maßnahmen werden ergriffen, um eine unangemessene Verwendung zu verhindern.

Folgende Personen haben Zugang zu den Bildern:

- Beamte und sonstige Bedienstete des Sicherheitsdienstes der Direktion Gebäude (Sichtung, Aufzeichnung, Vervielfältigung, Archivierung, Löschung);
- Bedienstete des Wachdienstes, die teilweise Sicherheitsaufgaben wahrnehmen (Sichtung in Echtzeit ohne Zugang zu den aufgezeichneten Bildern).

Die Bilder können in bestimmten Fällen an andere Empfänger übermittelt werden:

- den Gerichtshof, das Gericht der Europäischen Union (Gericht) und/oder das Gericht des öffentlichen Dienstes (GÖD) oder ein nationales Gericht sowie die Anwälte und Bevollmächtigten der Parteien im Fall eines Rechtsstreits;
- die mit der Prüfung von Beschwerden beauftragte Stelle des Gerichtshofs, des Gerichts oder des GÖD, den Präsidenten und den Kanzler des betreffenden Gerichts sowie den Rechtsberater für Verwaltungsangelegenheiten im Fall einer gemäß Art. 90 Abs. 2 des Beamtenstatuts eingelegten Beschwerde;
- Personen, die auf einen Sicherheitsvorfall hin im Rahmen einer von der Anstellungsbehörde oder der zum Abschluss von Dienstverträgen ermächtigten Behörde angeordneten Verwaltungsuntersuchung oder im Rahmen eines nach den Vorschriften des Anhangs IX des Statuts der Beamten der EU eröffneten Disziplinarverfahrens tätig werden;
- den Präsidenten und den Kanzler des Gerichtshofs sowie die Beamten, die sie im Rahmen der ihnen durch Art. 20 Abs. 4 der Verfahrensordnung des Gerichtshofs übertragenen Aufgaben unterstützen;
- den ESDB gemäß Art. 47 Abs. 2 der Verordnung Nr. 45/2001;
- den DSB des Organs gemäß Nr. 4 des Anhangs der Verordnung Nr. 45/2001;
- den Europäischen Bürgerbeauftragten, soweit dies für die Bearbeitung einer bei ihm eingereichten Beschwerde erforderlich ist (Art. 228 AEUV);
- das OLAF im Fall einer nach der Verordnung Nr. 883/2013 und dem Beschluss des Gerichtshofs vom 12. Juli 2011 über die Bedingungen und Modalitäten der internen Untersuchungen zur Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen zum Nachteil der Interessen der Europäischen Union durchgeführten Untersuchung.

Schließlich können die Bilder unter den in Art. 8 der Verordnung Nr. 45/2001 festgelegten Bedingungen den nationalen Behörden übermittelt werden, wenn sich dies als für eine in Ausübung ihrer Zuständigkeiten geführte Untersuchung erforderlich erweist.

Alle Datenübermittlungen werden in einem besonderen Register verzeichnet.

Personen, die zusätzliche Informationen erhalten oder ihre Rechte aus der Verordnung Nr. 45/2001 (Zugang, Berichtigung, Sperrung, Löschung oder Widerspruch) wahrnehmen möchten, kann sich an den Leiter des Sicherheitsdienstes wenden.

Die Art. 13 und 14 der Verordnung Nr. 45/2001, die das Auskunftsrecht und das Recht auf Berichtigung betreffen, sind nachstehend zitiert.

Die Person, deren personenbezogene Daten verarbeitet werden, hat gemäß Art. 32 Abs. 2 der Verordnung Nr. 45/2001 auch die Möglichkeit, sich an den ESBD zu wenden.

Art. 13 der Verordnung Nr. 45/2001

Auskunftsrecht

Die betroffene Person hat das Recht, jederzeit frei und ungehindert innerhalb von drei Monaten nach Eingang eines entsprechenden Antrags unentgeltlich von dem für die Verarbeitung Verantwortlichen folgende Auskünfte zu erhalten:
a) die Bestätigung, ob sie betreffende Daten verarbeitet werden oder nicht,
b) zumindest Angaben zu den Zwecken der Verarbeitung, den Datenkategorien, die verarbeitet werden, den Empfängern oder Kategorien von Empfängern, an die die Daten übermittelt werden,
c) eine Mitteilung in verständlicher Form über die Daten, die Gegenstand der Verarbeitung sind, sowie alle verfügbaren Informationen über die Herkunft der Daten,
d) Auskunft über den logischen Aufbau der automatisierten Verarbeitung der sie betreffenden Daten.

Art. 14 der Verordnung Nr. 45/2001

Berichtigung

Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen zu verlangen, dass unrichtige oder unvollständige personenbezogene Daten unverzüglich berichtigt werden.

2. Informationen über die verdeckte Videoüberwachung (Videoüberwachungsstrategie des Gerichtshofs der Europäischen Union, Nr. 4.4 „Verdeckte Videoüberwachung“)

Das Videoüberwachungssystem umfasst keine Geräte zur verdeckten Überwachung.

Im Rahmen einer internen Sicherheitsuntersuchung kann das Organ auf der Grundlage einer (dem Datenschutzbeauftragten zur Stellungnahme vorlegten) Folgenabschätzung und nach Beschluss des Kanzlers des Gerichtshofs im Ausnahmefall auf eine gesonderte verdeckte Videoüberwachung, die nicht mit dem allgemeinen Videoüberwachungssystem verbunden ist, zurückgreifen, um Personen zu ermitteln, die sich wiederholt unbefugt Zutritt verschafft, Diebstähle oder sonstige schwere Verstöße gegen Sicherheitsvorschriften begangen haben.

Die Folgenabschätzung muss belegen, wie die sich aus der Verwendung eines Systems der verdeckten Videoüberwachung ergebende Verletzung der Privatsphäre und des Schutzes der personenbezogenen Daten durch die mit der Verwendung dieses Systems verbundenen Vorteile ausgeglichen wird.
Hierzu berücksichtigt die Folgenabschätzung über die Garantien, die für den Einsatz der allgemeinen Videoüberwachung gelten, hinaus eine Reihe von Kriterien wie das Fehlen alternativer, privatsphärenfreundlicherer Maßnahmen und die für den Einsatz der entsprechenden Geräte vorgesehenen Grenzen (Ort, Uhrzeiten und Zeitraum des Einsatzes der Geräte, die sich nach den festgestellten Verstößen richten).

Die Geräte zur verdeckten Videoüberwachung können keinesfalls mit dem allgemeinen Videoüberwachungssystem verbunden werden. Daher werden die aufgezeichneten Bilder manuell erfasst.
Diese Bilder werden so bald als möglich, spätestens aber sieben Werktage nach der Aufzeichnung gesichtet, um ihre Erheblichkeit zu bewerten. Dieser Zeitraum von höchstens sieben Werktagen ist erforderlich, da tägliche Interventionen an den Geräten den störungsfreien Ablauf der internen Sicherheitsuntersuchung beeinträchtigen könnten, aber auch, um über genügend Zeit für die manuelle Erfassung der auf diesen Geräten befindlichen Bilder zu verfügen.

Die Bilder, die für die interne Sicherheitsuntersuchung nicht erheblich sind, werden unmittelbar nach ihrer ersten Sichtung gelöscht.
Die für die interne Sicherheitsuntersuchung erheblichen Bilder werden bis zum Abschluss dieser Untersuchung und der gegebenenfalls darauf folgenden Verfahren aufbewahrt.

Die auf den Bildern identifizierten Personen werden vom Sicherheitsdienst individuell unterrichtet, wenn mindestens eine der folgenden Bedingungen erfüllt ist:

- die Identität der Person wurde in einer Akte festgehalten;
- die Videoaufzeichnung wird gegen die Person verwendet;
- die Videoaufzeichnung wird über die oben vorgesehenen Zeiträume hinaus aufbewahrt;
- die Videoaufzeichnung wird an einen Empfänger außerhalb des Sicherheitsdienstes übermittelt oder
- die Identität der Person wird einer Person außerhalb des Sicherheitsdienstes mitgeteilt.

Diese Unterrichtung kann aufgeschoben werden, wenn dies für die interne Sicherheitsuntersuchung erforderlich ist, oder in anderen, in Art. 20 der Verordnung Nr. 45/2001 (nachstehend zitiert) vorgesehenen Fällen.

Art. 20 der Verordnung Nr. 45/2001

Ausnahmen und Einschränkungen

(1) Die Organe und Einrichtungen der Gemeinschaft können die Anwendung von Artikel 4 Absatz 1, Artikel 11, Artikel 12 Absatz 1, Artikel 13 bis 17 und Artikel 37 Absatz 1 insoweit einschränken, als eine solche Einschränkung notwendig ist für

a) die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten;

b) ein wichtiges wirtschaftliches oder finanzielles Interesse eines Mitgliedstaats oder der Europäischen Gemeinschaften, einschließlich Währungs-, Haushalts- oder Steuerangelegenheiten;

c) den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen;

d) die nationale und die öffentliche Sicherheit sowie die Verteidigung der Mitgliedstaaten;

e) Kontroll-, Überwachungs- und Ordnungsaufgaben, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt in den unter den Buchstaben a) und b) genannten Fällen verbunden sind.

(2) Die Artikel 13 bis 16 finden keine Anwendung, wenn Daten ausschließlich für Zwecke der wissenschaftlichen Forschung verarbeitet oder personenbezogen nicht länger als lediglich zur Erstellung von Statistiken erforderlich aufbewahrt werden, sofern offensichtlich keine Gefahr eines Eingriffs in die Privatsphäre der betroffenen Person besteht und der für die Verarbeitung Verantwortliche angemessene rechtliche Garantien vorsieht, insbesondere dass die Daten nicht für Maßnahmen oder Entscheidungen gegenüber bestimmten Personen verwendet werden.

(3) Findet eine Einschränkung nach Absatz 1 Anwendung, ist die betroffene Person gemäß dem Gemeinschaftsrecht über die wesentlichen Gründe für diese Einschränkung und darüber zu unterrichten, dass sie das Recht hat, sich an den Europäischen Datenschutzbeauftragten zu wenden.

(4) Wird eine Einschränkung nach Absatz 1 angewandt, um der betroffenen Person den Zugang zu verweigern, unterrichtet der Europäische Datenschutzbeauftragte bei Prüfung der Beschwerde die betroffene Person nur darüber, ob die Daten richtig verarbeitet wurden und, falls dies nicht der Fall ist, ob alle erforderlichen Berichtigungen vorgenommen wurden.

(5) Die Unterrichtung nach den Absätzen 3 und 4 kann so lange aufgeschoben werden, wie sie die Einschränkung gemäß Absatz 1 ihrer Wirkung beraubt.