Het beleid van het Europees Parlement inzake cameratoezicht

vastgesteld door de adjunct-secretaris-generaal van het Europees Parlement

Mw. Francesca R. RATTI

20 april 2013

Inhoudsopgave

1. Doel en reikwijdte van het beleid inzake cameratoezicht

Het Europees Parlement (hierna het EP genoemd) heeft de beschikking over een operatief systeem voor cameratoezicht voor het voorkomen, ontmoedigen, beheersen en onderzoeken van veiligheids- en beveiligingsincidenten, alsmede voor de bescherming van personen, eigendommen en documenten tegen brand, diefstal, indringing, aanslagen en eventuele andere bedreigingen. Door het toezicht op bepaalde ruimten en evenementen is het systeem voor cameratoezicht een aanvulling op de andere methodes die specifiek op de beveiliging en de toegangscontrole gericht zijn. Het maakt deel uit van de maatregelen die het bredere veiligheidsbeleid van het EP ondersteunen.

Het Directoraat veiligheid en risicobeoordeling binnen DG Presidium is verantwoordelijk voor de verwerking van de gegevens afkomstig van het cameratoezicht.

Deze nota over het beleid inzake het cameratoezicht bevat een beschrijving van het systeem van het EP voor het cameratoezicht, het doel en het gebruik daarvan, alsmede de voorzorgsmaatregelen die het EP neemt ter bescherming van de persoonsgegevens en de privacy van degenen binnen het EP en in de directe omgeving daarvan.

De onderdelen van dit toezichtbeleid gelden op de drie werklocaties van het Europees Parlement, in Luxemburg, Straatsburg en Brussel.

2. Hoe waarborgen wij dat ons systeem voor cameratoezicht ontworpen is indachtig de privacy- en gegevensbescherming en voldoet aan de gegevensbeschermingswetgeving?

2.1. Herziening van het bestaande systeem

Het EP had reeds de beschikking over een systeem voor cameratoezicht toen de Europese Toezichthouder voor gegevensbescherming in maart 2010 de richtsnoeren voor cameratoezicht (hierna "de richtsnoeren") deed uitgaan. De procedures van het EP worden echter regelmatig herzien om te voldoen aan de aanbevelingen die in de richtsnoeren vastgelegd zijn (in hoofdstuk 15), en om de gegevensbeschermingsnormen binnen het EP te verbeteren.

De richtsnoeren van de Europese toezichthouder voor gegevensbescherming (EDPS) zijn online te vinden op:
http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/Guidelines

2.2. Naleving

De beelden worden door het Parlement verwerkt in overeenstemming met zowel de richtsnoeren als Verordening (EG) nr. 45/2001 inzake de verwerking van persoonsgegevens door de communautaire instellingen en organen.

2.3. Controle op het gesloten tv-circuitsysteem en de gegevensbeschermings in eigen beheer

Het gesloten tv-circuitsysteem (CCTV) van het EP werd onderworpen aan een complete controle in eigen beheer van elke afzonderlijke camera. Voor elke camera werd een risicoanalyse (inzake beveiliging en veiligheid) en een effectbeoordeling (inzake gegevensbescherming) uitgevoerd. Op basis van de beide analyses en overeenkomstig de doelstelling om het toezicht op de ruimten die niet relevant zijn voor de voorziene doeleinden zoveel mogelijk te beperken, werden de cameralocaties en -hoeken gewijzigd, opgeheven of bevestigd.

Bovendien is er een grondige controle uitgevoerd van de huidige stand van zaken om na te gaan of de gegevensbeschermingspraktijken in verband met het cameratoezicht van de EP geschikt zijn en voldoen aan de bepalingen van de verordening en de richtsnoeren. Aangezien er voorheen geen beleid bestond inzake het cameratoezicht heeft deze controle geresulteerd in dit beleid.

2.4. Kennisgeving inzake de naleving van de richtsnoeren aan de EDPS

Indien er een systeem voor cameratoezicht geïnstalleerd of ingrijpend gewijzigd wordt, zal het directoraat Veiligheid en Risicobeoordeling (DV), bijgestaan door de functionaris voor gegevensbescherming (DPO) van het EP, een formele privacyeffectbeoordeling maken en zo nodig voorafgaand een kennisgeving doen toekomen aan de EDPS.

Deze nota over het beleid inzake het cameratoezicht en iedere belangrijke herziening worden aan de EDPS gezonden. De kennisgeving met betrekking tot de naleving inzake het cameratoezicht door het EP bestaat uit dergelijke uitwisselingen met de EDPS.

2.5. Contacten met de relevante gegevensbeschermingsautoriteiten in de lidstaten

Na de goedkeuring is dit beleidsdocument naar de relevante autoriteiten in België, Frankrijk en Luxemburg gestuurd. Bij toekomstige herzieningen van dit beleid zal rekening gehouden worden met de eventuele op- en aanmerkingen van deze autoriteiten.

2.6. Besluitvorming en raadpleging

De besluiten om het bestaande systeem voor cameratoezicht te handhaven, de bestaande praktijken te controleren, gerichte, specifieke aanpassingen ter verdere verbetering van het nalevingsniveau te benoemen en de waarborgen vast te leggen zoals ze beschreven zijn in dit beleid inzake het cameratoezicht, zijn genomen door de autoriteiten van het EP na raadpleging van:

- de functionaris voor gegevensbescherming van het EP en
- de Europese toezichthouder voor gegevensbescherming.

Gedurende dit besluitvormingsproces heeft het EP:

- de noodzaak aangetoond van een systeem voor cameratoezicht zoals dat in dit beleid voorgesteld wordt;
- zich ervan vergewist dat de doeleinden daarvan legitiem zijn;

- alternatieven besproken en geconcludeerd dat het gebruik van het huidige systeem voor cameratoezicht, na vastlegging van de in dit beleid voorgestelde waarborgen inzake gegevensbescherming, noodzakelijk en proportioneel is voor de onder punt 1 genoemde doeleinden (zie hierboven);
- zich gebogen over de door de geraadpleegde organisaties geuite bezwaren.

Met betrekking tot dit beleid inzake cameratoezicht zullen andere belanghebbenden, waaronder het personeelscomité van het EP, via het EP-netwerk van veiligheidscorrespondenten benaderd worden, en bij de verdere ontwikkeling van dit beleid zal rekening gehouden worden met eventueel commentaar.

2.7 Transparantie

Er bestaan twee versies van dit beleid inzake het cameratoezicht, één voor beperkt gebruik en deze versie die voor het publiek toegankelijk is gemaakt op onze internet- en intranetpagina's.

Het kan zijn dat deze publieksversie van het beleid inzake cameratoezicht ten aanzien van bepaalde onderwerpen summiere informatie bevat. Er is alleen informatie weggelaten uit de publieksversie indien dit om dwingende redenen absoluut noodzakelijk is voor de geheimhouding (bij voorbeeld om veiligheidsredenen, om vertrouwelijke en gevoelige informatie af te schermen of om de privacy van personen te beschermen).

2.8. Periodieke evaluaties

Iedere twee jaar zal er een periodieke gegevensbeschermingsevaluatie gemaakt worden door het Directoraat veiligheid en risicobeoordeling. Tijdens die periodieke evaluatie zal het DV beoordelen of:

- er nog steeds behoefte is aan het systeem voor cameratoezicht;
- het systeem nog dienstig is aan de gestelde doeleinden;
- er nog steeds geen adequate alternatieven voorhanden zijn.

De periodieke evaluaties zullen ook ingaan op andere kwesties die in het eerste controleverslag behandeld worden, met name op de vraag of ons beleid inzake cameratoezicht nog steeds voldoet aan de verordening en de richtsnoeren (geschiktheidscontrole), en of dit in de praktijk wordt nageleefd (nalevingscontrole).

2.9. Privacyvriendelijke technologische oplossingen

Bij het bestellen van nieuwe apparatuur voor het systeem en bij elke andere zich aandienende gelegenheid, zal het EP gebruikmaken van de beste privacyvriendelijke technologische oplossingen die voorhanden zijn.

Op basis van een risicoanalyse en privacyeffectbeoordeling is het EP al bezig met het uitvoeren en verbeteren van privacyvriendelijke technologische en procedurele oplossingen, zoals:

- bewegingsdetectie;
- beperkte toegang tot het systeem;
- cameraresoluties op basis van risico (de resolutie is zo laag als mogelijk is bij de voorgenomen veiligheidsdoelstelling).

3. Welke ruimten staan onder toezicht?

De cameralocaties en -hoeken zijn gebaseerd op een methodologische risicoanalyse en privacyeffectbeoordeling, waarbij gewaarborgd wordt dat de camera's alleen gericht zijn op de meest relevante locaties binnen en buiten de gebouwen (zie punt 2.3 hierboven).

De camera's zijn geïnstalleerd om toezicht te houden op de in- en uitgangen van de gebouwen (de hoofdingangen, de nood- en branduitgangen en de toegang tot de parkeerfaciliteiten). Bovendien zijn er camera's voor het toezicht op verscheidene belangrijke trappenhuizen of verbindingspunten en in de nabijheid van bijzondere ruimten die extra beveiliging behoeven, zoals die waar grote hoeveelheden geld bewaard worden, gevoelige vergaderingen gehouden worden of beperkte toegang geldt.

Wij houden geen toezicht op ruimten waarin men een hoge mate van privacy mag verwachten, zoals individuele bureauruimten, ontspanningsruimten of toiletfaciliteiten.

Op het grondgebied van België, Luxemburg en Frankrijk blijft het toezicht beperkt tot een zo smal mogelijke zone rondom onze gebouwen.

4. Welke persoonsgegevens worden voor welke doeleinden verzameld?

4.1. Technische specificaties van het systeem

Het systeem voor cameratoezicht van het EP is een conventioneel systeem. Alle camera's zijn 24 uur per dag operationeel, gedurende zeven dagen in de week. De beeldkwaliteit is in de meeste gevallen van dien aard dat de identificatie van degenen die zich in de door de camera's bestreken ruimte bevinden mogelijk is. Het systeem neemt digitale beelden op en is uitgerust met bewegingsdetectie. Iedere beweging die door de camera's in de ruimte die onder toezicht staat wordt waargenomen, wordt onder vermelding van het tijdstip, de datum en de locatie opgenomen.

Wij maken geen gebruik van geavanceerde of intelligente technologie voor het cameratoezicht, wij koppelen ons systeem niet aan andere systemen en wij gebruiken geen geluidsopnames of een "gesloten audiotelevisiecircuit" (de richtsnoeren 6.12).

4.2. Doeleinden van het toezicht

Het Europees Parlement gebruikt zijn videobewakingssysteem ten behoeve van de veiligheid, de beveiliging en de toegangscontrole. Het cameratoezicht levert een bijdrage aan de controle op de toegang tot onze gebouwen en aan het verzekeren van de beveiliging en de veiligheid van onze gebouwen, de parlementsleden, het personeel en de bezoekers, alsmede van de in de gebouwen aanwezige of opgeslagen eigendommen en documenten.

Het systeem voor cameratoezicht helpt bij het voorkomen, ontmoedigen, beheersen en, waar nodig, onderzoeken van aan veiligheid en beveiliging gerelateerde incidenten, mogelijke dreigingen en ongeoorloofde fysieke toegang, inclusief het zich op ongeoorloofde wijze toegang verschaffen tot beveiligde gebouwen en beschermde ruimten, IT-infrastructuur en operationele informatie.

Regelmatig uitgevoerde risicoanalyses in het kader van het algemene veiligheidsconcept van het EP bevestigen dat cameratoezicht helpt bij het voorkomen, ontdekken en onderzoeken van diefstal van apparatuur en bezittingen van het EP, de parlementsleden, het personeel, de contractanten of bezoekers, alsmede van bedreigingen van de veiligheid binnen de gebouwen.

4.3. Doelbeperking

Het systeem wordt niet voor andere doeleinden gebruikt dan de voornoemde. Zo wordt het bijvoorbeeld niet gebruikt om het werk van medewerkers of hun aanwezigheid te controleren. Het systeem wordt evenmin ingezet als onderzoeksinstrument voor andere doeleinden dan bij de hierboven beschreven gevallen, noch in het kader van tuchtrechtelijke procedures, tenzij er sprake is van een incident waarbij de lichamelijke veiligheid in het geding is, of van crimineel gedrag.

Alleen onder uitzonderlijke omstandigheden mogen er opnames overgedragen worden aan onderzoeksinstanties in het kader van een officieel tuchtrechtelijk of strafrechtelijk onderzoek, zoals hieronder in punt 6.5 beschreven is.

4.4. Speciale en heimelijke observaties

Er bestaat geen basis voor speciale observatieoperaties binnen het kader van het CCTV-systeem. In uitzonderlijke gevallen en helemaal buiten het CCTV-systeem om, kan het EP evenwel voor een beperkte tijdsduur gebruikmaken van op zichzelf staande heimelijke observaties tijdens interne onderzoeken. De hiervoor bestemde camera's worden onder strikte voorwaarden geplaatst om ervoor te zorgen dat de aantasting van de privacy tot een minimum beperkt blijft.

Indien er in specifieke gevallen twijfel bestaat over kwesties inzake gegevensbescherming, zal de DPO geraadpleegd worden.

4.5. Webcams

Het EP maakt geen gebruik van webcams voor beveiligings- of veiligheidsdoeleinden.

4.6. Speciale categorieën gegevens

Het systeem voor cameratoezicht van het EP is niet gericht op het verzamelen van speciale categorieën gegevens, zoals raciale of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, vakbondslidmaatschap of gegevens met betrekking tot de gezondheid of seksuele oriëntatie.

Via het CCTV-systeem wordt het kleinst mogelijke gebied geobserveerd dat noodzakelijk is om de veiligheid en de beveiliging van de gebouwen te garanderen. Gezien het hoge veiligheidsrisiconiveau van de gebouwen van het EP (het

omliggende terrein is gemakkelijk toegankelijk), zijn alle toegangen en de directe omtrek van het Europees Parlement uitgerust met camera's. Het gebruik van deze camera's is niet bedoeld om speciale categorieën gegevens vast te leggen of te verwerken, noch om individuen te observeren, maar om in staat te zijn veiligheidsgerelateerde incidenten te voorkomen, te beoordelen en te onderzoeken. Degenen die deze speciale camera's bedienen, krijgen een opleiding inzake gegevensbescherming en grondrechten.

5. Wat is de rechtsgrondslag en de juridische basis van dit cameratoezicht?

Het gebruik van ons systeem van cameratoezicht is noodzakelijk voor het beheer en de werking van het EP (voor veiligheid, beveiliging en toegangscontrole, zie punt 4.2 hierboven), zoals vastgelegd is het besluit van het Bureau van het EP van 16 december 2002 en, meer in algemene zin, in de besluiten van het Bureau van het EP van 3 mei 2004 en 6 juli 2011.

Dit beleid inzake het cameratoezicht maakt op zijn beurt deel uit van algemenere uitvoeringsregelgeving en wordt als zodanig regelmatig bijgewerkt of aangepast in overeenstemming met eventuele specifieke dreigingen, politieke omstandigheden of technische mogelijkheden.

In het licht van het bovenstaande beschikt het EP over een juridische basis en een reeks duidelijke procedures voor zijn systeem van cameratoezicht.

6. Voor wie is deze informatie toegankelijk en wie wordt ervan in kennis gesteld?

6.1. Eigen en extern beveiligings- en onderhoudspersoneel

Het uitvoeren van het cameratoezicht wordt voor een gedeelte door het EP uitbesteed.

Live-videobeelden zijn toegankelijk voor dienstdoend beveiligingspersoneel dat voor een extern beveiligingsbedrijf werkt, indien dit voor de uitvoering van hun taken noodzakelijk is ("need to know"). Externe medewerkers hebben alleen toegang tot opgeslagen beeldmateriaal indien zij daarvoor uitdrukkelijke toestemming hebben van het hoofd van de afdeling Risicobeheer of Interne Veiligheid.

Het computersysteem van het CCTV staat niet toe dat externe medewerkers beeldmateriaal opslaan op externe media (zoals een DVD-schijf of USB-stick). Het uitvoeren van dit soort handelingen die te allen tijde geregistreerd dienen te worden, is uitsluitend voorbehouden aan EP-functionarissen van het DV.

Het onderhoud van het systeem voor cameratoezicht wordt eveneens uitgevoerd door een contractant onder supervisie van een veiligheidsfunctionaris van het EP.

De verplichtingen van beide contractanten (voor de veiligheid en het onderhoud) ten aanzien van gegevensbescherming zijn op een juridische bindende wijze schriftelijk

vastgelegd. Tevens dienen de contractanten te zorgen voor passende opleidingen inzake gegevensbescherming voor hun personeel.

6.2. Toegangsrechten

In het document over het beveiligingsbeleid van het EP voor cameratoezicht is gespecificeerd en vastgelegd wie er toegang hebben tot het beeldmateriaal van de camera's voor het toezicht en/of de technische structuur van het systeem voor cameratoezicht, voor welke doeleinden en waar deze toegangsrechten uit bestaan. In het bijzonder wordt in dit document gespecificeerd wie het recht heeft om:

- de live-beelden te zien;
- het opgenomen beeldmateriaal te bekijken;
- kopieën te maken;
- te downloaden;
- te wissen;
- beeldmateriaal te veranderen.

6.3. Opleidingen inzake gegevensbescherming

Al het personeel dat over toegangsrechten beschikt, met inbegrip van externe beveiligers en onderhoudstechnici, krijgen opleidingen inzake gegevensbescherming. Ieder nieuw personeelslid krijgt een opleiding en tenminste iedere twee jaar worden er voor alle personeelsleden met toegangsrecht workshops gegeven over kwesties inzake de naleving van de voorschriften inzake gegevensbescherming.

6.4. Geheimhoudingsgelofte

Personeelsleden met toegangsrechten, met inbegrip van het ingehuurde personeel dat dagelijks het CCTV-toezicht of het onderhoud van het systeem uitvoert, ondertekenen een geheimhoudingsgelofte om ervoor te zorgen dat zij de inhoud van het beeldmateriaal van het cameratoezicht aan niemand anders dan de gemachtigde ontvangers overdragen, laten zien of op enige andere wijze openbaar maken.

6.5. Overdracht, openbaarmaking en registratie

De verzamelde informatie die afkomstig is van de verwerking van persoonsgegevens, met inbegrip van CCTV-beeldmateriaal, kan openbaar worden gemaakt aan de veiligheidsdiensten van andere Europese instellingen of aan veiligheids-, rechts- of wetshandhavingsinstanties van EU-lidstaten ten behoeve van lopend onderzoek of met het oog op onderzoek naar en vervolging van misdrijven. Een dergelijke overdracht kan alleen op verzoek plaatsvinden. Er is geen sprake van een geregelde of routinematige overdracht.

Elke overdracht of openbaarmaking aan instanties buiten het Directoraat veiligheid en risicobeoordeling wordt onderworpen aan een strenge beoordeling van de noodzaak van overdracht en wordt terdege gedocumenteerd.

Noch de directie, noch de dienst personeelszaken krijgt toegang tot het CCTV-systeem voor andere dan de in dit beleid beschreven doeleinden.

De noodzaak om gebruik te maken van opgenomen beeldmateriaal (zie punt 4.2 hierboven) kan de betrokkenheid vereisen van twee afdelingen van het directoraat, namelijk de afdelingen Risicobeheer en Interne Veiligheid. Elke afdeling is verantwoordelijk voor de naleving van de in dit beleid vermelde procedures en gegevensbeschermingsvoorschriften, alsmede de kennisgevingen van het directoraat aan de DPO, en elke afdeling houdt haar eigen register bij, zoals in dit beleid beschreven.

- De afdeling Interne Veiligheid beheert een register van de opnamen die na de bewaartermijnen bewaard worden.

- De afdeling Risicobeheer houdt een register bij van de opnamen die na de bewaartermijnen bewaard worden en van de gevallen van overdracht en openbaarmakingen aan derde partijen.

7. Hoe beveiligen en waarborgen wij de informatie?

Ten einde de veiligheid van het systeem voor cameratoezicht in zijn geheel te beschermen, met inbegrip van de persoonsgegevens, worden er een aantal technische en organisatorische maatregelen herzien en geleidelijk aan ingevoerd.

Zij worden gedetailleerd beschreven in een beveiligingsbeleid voor cameratoezicht dat specifiek gericht is op de verwerking. Het beveiligingsbeleid van het EP voor cameratoezicht is vastgesteld in overeenstemming met hoofdstuk 9 van de EDPS-richtsnoeren voor cameratoezicht.

Alle mogelijke technische en fysieke maatregelen worden genomen om te garanderen dat het systeem beveiligd is en de gegevens beschermd zijn, waaronder:

- het personeel (zowel het externe als het interne) ondertekent een niet-openbaarmakings- en geheimhoudingsovereenkomst;
- gebruikers krijgen slechts toegang tot die middelen die strikt noodzakelijk zijn voor de uitvoering van hun taken (op basis van het "need to know"-beginsel);
- het beveiligingsbeleid voor cameratoezicht bevat een bijgewerkte lijst van alle functies/posten die te allen tijde recht geven op toegang tot het systeem en beschrijft deze toegangsrechten.

8. Hoe lang bewaren we de gegevens?

Op basis van een risicoanalyse en een privacyeffectbeoordeling wordt voor elke afzonderlijke camera een besluit genomen over de bewaartermijn, die normaliter maximaal twee maanden mag zijn. Deze verlengde bewaartermijn is van essentieel belang voor onderzoeksdoeleinden, aangezien er in veel gevallen pas na lange tijd een klacht wordt ingediend, als gevolg van het feit dat de gebruikers op verschillende werklocaties aanwezig zijn.

Als beelden moeten worden opgeslagen als bewijs van een veiligheidsincident of om het incident verder te onderzoeken, mogen zij voor de duur van het onderzoek worden bewaard en kunnen zij, zo nodig, samen met de onderzoeksresultaten maximaal tien jaar worden gearchiveerd. Het bewaren van beelden wordt uitvoerig gedocumenteerd.

9. Hoe verschaffen wij het publiek informatie?

9.1. De gelaagde aanpak

Wij verschaffen het publiek (degenen die de directe omgeving en/of de gebouwen of de toegangen tot de parkeerfaciliteiten van het EP betreden) op een doelmatige en begrijpelijke manier informatie over het cameratoezicht. Hiervoor maken wij gebruik van een gelaagde aanpak die bestaat uit een combinatie van de volgende drie methoden:

- kennisgevingen ter plekke om het publiek (voetgangers, automobilisten, bezoekers, personeel, enz.) attent te maken op het feit dat er toezicht plaatsvindt en essentiële informatie te verschaffen met betrekking tot de verwerking daarvan;
- de beschikbaarheid van een samenvatting van dit beleidsdocument bij de ontvangstbalies;
- de beschikbaarheid van dit beleidsdocument op ons intranet en ons internet voor degenen die meer willen weten over het cameratoezicht dat onze instelling hanteert.

Voor verdere vragen en informatie over het verhaalsrecht wordt er een e-mailadres aangegeven.

9.2. Specifieke persoonlijke kennisgeving

Personen ontvangen ook een persoonlijke kennisgeving indien zij op basis van beeldmateriaal geïdentificeerd zijn (bijvoorbeeld door beveiligingspersoneel in het kader van een beveiligingsonderzoek), vooropgesteld dat wordt voldaan aan één of meer van de volgende voorwaarden:

- hun identiteit staat in een dossier vermeld;
- de gegevens omtrent hun identiteit worden langer dan de bewaartermijn bewaard;
- het beeldmateriaal wordt gebruikt tegen de persoon;
- er is sprake van een overdracht van het beeldmateriaal buiten het DV;
- de identiteit van de persoon wordt aan een instantie of persoon buiten het DV bekend gemaakt.

Er kan echter worden afgezien van een individuele kennisgeving of deze kan tijdelijk uitgesteld worden zolang dat noodzakelijk wordt geacht in verband met beveiligings- of veilgheidsredenen, bijvoorbeeld om mogelijke strafbare feiten, terroristische daden of andere uitzonderingen als bedoeld in artikel 20 van de verordening te voorkomen, te onderzoeken, te ontdekken en te vervolgen.

Indien een dergelijke situatie zich voordoet en in het geval van twijfel ten aanzien van de inachtneming van het recht op bescherming van persoonsgegevens zal het directoraat Veiligheid relevant advies inwinnen bij de DPO.

10. Hoe kan het publiek zijn gegevens controleren, aanpassen of wissen?

Het publiek heeft het recht om de door ons bewaarde persoonsgegevens in te zien en deze gegevens te corrigeren en aan te vullen. Elk verzoek om inzage in en het corrigeren, blokkeren en/of wissen van persoonsgegevens moet worden gericht aan:

Europees Parlement
Directoraat Veiligheid en Risicobeoordeling
Wiertzstraat 60
B-1047 Brussel
E-mail: Securite-ProtectionDonnees@ep.europa.eu
Telefoon: +32 2 28 42040
Fax: +32 2 28 41674

Het directoraat Veiligheid en Risicobeoordeling kan ook benaderd worden voor andere vragen met betrekking tot de verwerking van persoonsgegevens.

Het directoraat Veiligheid en Risicobeoordeling beantwoordt een verzoek inhoudelijk binnen 15 kalenderdagen. Indien dit niet mogelijk is, wordt de aanvrager binnen 15 dagen over het vervolg en de redenen van het uitstel geïnformeerd. Zelfs in de meest gecompliceerde gevallen wordt er binnen hoogstens drie maanden toestemming voor inzage of een met redenen omkleed definitief antwoord ter afwijzing van het verzoek gegeven. De diensten zullen hun best doen om eerder te reageren, vooral indien de aanvrager duidelijk maakt dat het een urgent verzoek betreft.

Indien hierom specifiek verzocht is, kan er geregeld worden dat de aanvrager het beeldmateriaal te zien krijgt of kan deze een kopie verkrijgen van de opgenomen beelden. Bij een dergelijk verzoek dienen de aanvragers hun identiteit zonder enige ruimte voor twijfel aan te tonen (zij moeten bijvoorbeeld een identiteitskaart meebrengen om de beelden te kunnen bekijken) en zo mogelijk de datum, tijd, locatie en omstandigheden aangeven van de gelegenheid waarbij ze door de camera's vastgelegd werden. Zij dienen ook een recente foto van zichzelf te verstrekken, zodat het beveiligingspersoneel hen van de afgespeelde beelden kan herkennen.

Momenteel brengen wij de aanvragers geen kosten in rekening voor het tonen of kopiëren van het opgenomen beeldmateriaal. Wij behouden ons echter het recht voor om een redelijk bedrag in rekening te brengen indien het aantal verzoeken om inzage toeneemt.

Een verzoek om inzage kan geweigerd worden indien er in een specifiek geval sprake is van een uitzondering uit hoofde van artikel 20, lid 1, van Verordening (EG) nr. 45/2001 (zie ook punt 9.2 hierboven). Het is bijvoorbeeld mogelijk dat wij, aan de hand van een beoordeling van het afzonderlijke geval, moeten concluderen dat de inperking van het inzagerecht noodzakelijk is ter bescherming van een onderzoek naar een strafbaar feit. Een inperking kan ook noodzakelijk zijn om de rechten en vrijheden van anderen te beschermen als er bijvoorbeeld andere personen aanwezig zijn op het beeldmateriaal en het niet mogelijk is hun toestemming te verkrijgen om hun persoonsgegevens openbaar te maken of beeldmontage te gebruiken om het ontbreken van toestemming te ondervangen.

11. Verhaalsrecht

Ieder persoon heeft het recht om verhaal te halen bij de Europese Toezichthouder voor gegevensbescherming via het e-mailadres edps@edps.europa.eu, indien hij/zij van mening is dat er inbreuk gemaakt is op zijn/haar rechten krachtens Verordening (EG) nr. 45/2001 als gevolg van de verwerking van zijn/haar persoonsgegevens door het Europees Parlement. Alvorens dit te doen, bevelen wij aan dat men eerst verhaal probeert te halen door contact op te nemen met:

- De verantwoordelijke bij het Europees Parlement voor gegevensverwerking
  Directoraat Veiligheid en Risicobeoordeling
  E-mail: Securite-ProtectionDonnees@ep.europa.eu

en/of

- Functionaris voor gegevensbescherming bij het Europees Parlement
  Tel.: +352 4300 23595
  E-mail: data-protection@ep.europa.eu

Personeelsleden mogen ook een herzieningsverzoek indienen bij hun tot aanstelling bevoegd gezag uit hoofde van artikel 90 van het personeelsstatuut.