rijksuniversiteit groningen

Beleid cameratoezicht Rijksuniversiteit Groningen 23 mei 2025

Samenvatting

Op de terreinen en in en om de gebouwen van de Rijksuniversiteit Groningen (hierna: **RUG**) wordt gebruikgemaakt van cameratoezicht. De beeld- en audioinformatie en andere gegevens die met dit toezicht worden verkregen, kunnen persoonsgegevens bevatten. Cameratoezicht maakt daarom inbreuk op de persoonlijke levenssfeer van studenten, medewerkers en bezoekers. De RUG moet zich daarom bij het verwerken van dit soort informatie houden aan de Algemene Verordening Gegevensbescherming (hierna: **AVG**) en andere toepasselijke wet- en regelgeving.

Het inzetten van cameratoezicht is voor de RUG een noodzakelijke maatregel om:
- de veiligheid van medewerkers, studenten en bezoekers op haar terreinen en in haar gebouwen te beschermen;
- haar terreinen, gebouwen en andere opstallen te beveiligen en beschadiging daarvan te voorkomen of te detecteren;
- de zaken die zich op haar terreinen of in haar opstallen bevinden te bewaken; en
- incidenten te voorkomen en te detecteren.

De RUG maakt alleen gebruik van cameratoezicht als dit noodzakelijk is, proportioneel is en minder ingrijpende maatregelen niet effectief zijn (subsidiariteit). Dit wordt per locatie beoordeeld en periodiek geëvalueerd.

Het doel van dit beleid is het bevorderen en waarborgen dat:
- de RUG de wet- en regelgeving die van toepassing is op cameratoezicht naleeft;
- cameratoezicht wordt ingezet voor bovenstaande doelen;
- de interne verantwoordelijkheden voor het besluit tot- en de uitvoering van cameratoezicht helder zijn;
- studenten, medewerkers en bezoekers voldoende zijn geïnformeerd over de wijze waarop de RUG omgaat met cameratoezicht.

Het beleid geeft een beschrijving van de taken, verantwoordelijkheden en procedures binnen de RUG en omschrijft op welke wijze betrokkenen hun rechten kunnen uitoefenen.

Artikel 1. Begripsbepalingen

In dit beleid wordt verstaan onder:

a. **Analysegegevens**: gegevens, waaronder Persoonsgegevens, die met behulp van het Camerasysteem worden gegenereerd op basis van/over de Opnamen, zoals gegevens die worden verwerkt over aantallen personen in een ruimte.
b. **Betrokkene**: de natuurlijke persoon, als bedoeld in artikel 4 sub 1 AVG, van wie Persoonsgegevens (kunnen) worden verwerkt bij het uitvoeren van Cameratoezicht. Een betrokkene kan bijvoorbeeld een student, medewerker of bezoeker van de terreinen en/of gebouwen van de RUG zijn.
c. **Camerasysteem**: het geheel van camera's, weergaveapparatuur en ondersteunende hard- en software dat gebruikt wordt om Cameratoezicht uit te voeren.
d. **Cameratoezicht**: het maken van Opnamen met camera's van personen, terreinen, opstallen en/of zaken ten behoeve van de hieronder in artikel 3 beschreven doeleinden.
e. **Directeur Vastgoedorganisatie**: de directeur van de vastgoedorganisatie van de RUG, onderdeel van University Services, Cluster Campus & Community.
f. **DPIA**: Data Protection Impact Assessment (Gegevensbeschermingseffectbeoordeling) als bedoeld in artikel 35 AVG.
g. **Heimelijk Cameratoezicht:** het verrichten van Cameratoezicht met verborgen camera's, zonder de Betrokkene te informeren voorafgaand aan of tijdens dat toezicht.
h. **Hoofd Bestuurlijke en Juridische Zaken**: het Hoofd van de afdeling Bestuurlijke en Juridische Zaken, onderdeel van University Services, Stafafdeling Governance & Legal.
i. **Incident**: voorval dat lijkt te wijzen op strafbaar, onrechtmatig of verboden handelen van personen of een voorval dat leidt tot beschadiging aan of ongeoorloofd gebruik van een terreinen en opstallen van de RUG of zaken van de RUG of derden.
j. **Locatie**: het terrein en de gebouwen en/of andere opstellen waarop en/of waarbinnen Cameratoezicht wordt gehouden.
k. **Opnamen**: de door het cameratoezicht verkregen, *live* of na vastlegging waar te nemen, video- en/of audio-opnamen, waaronder de Persoonsgegevens die de opnamen bevatten.
l. **Persoonsgegevens**: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de Betrokkene), als bedoeld in artikel 4 sub 1 AVG.
m. **RUG:** Rijksuniversiteit Groningen.
n. **Security Manager**: de security manager van de RUG, tevens het Hoofd van de Fysieke beveiligingsorganisatie van de RUG, onderdeel van University Services, Cluster Campus & Community, afdeling clustersupport.
o. **Verwerking**: elke handeling of ieder geheel van handelingen met betrekking tot de Opnamen, Persoonsgegevens en Analysegegevens, waaronder verwerking als bedoeld in artikel 4 sub 2 AVG.

Artikel 2. Toepassingsbereik

1. Dit beleid geldt voor alle Locaties waar de RUG gebruikmaakt van Cameratoezicht en heeft betrekking op elke Verwerking. Dit beleid is een richtlijn als bedoeld in paragraaf 3.14 van het Algemeen Beleid Bescherming Persoonsgegevens van de RUG.[1] Bij tegenstrijdigheden tussen deze twee beleidsdocumenten prevaleert dit beleid cameratoezicht.
2. Dit beleid is niet van toepassing op:
   a. Gebruik van camera's ten behoeve van het registreren en uitzenden van colleges, academische plechtigheden en andere bijeenkomsten;
   b. Gebruik van camera's ten behoeve van het voeren van overleg;
   c. Verwerking van videobeelden en audiomateriaal in het kader van wetenschappelijk onderzoek;
   d. Gebruik van camera's ten behoeve van surveillance bij (online) tentamens en examens.
   e. Cameratoezicht in opstallen of op terreinen van de RUG die niet door de RUG zelf worden gebruikt, bijvoorbeeld omdat de RUG deze verhuurt.
   f. Het voor bedrijfsvoeringsdoeleinden gebruiken van procescamera's waarmee Opnamen of Analysegegevens worden vervaardigd die geen Persoonsgegevens bevatten.

Artikel 3. Doeleinden

1. Cameratoezicht en de Verwerking van Opnamen geschiedt uitsluitend ten behoeve van de volgende doeleinden:
   a. het beschermen van de veiligheid van medewerkers, studenten en bezoekers op de terreinen en in de gebouwen van de RUG;
   b. het beveiligen van de terreinen, gebouwen en andere opstallen van de RUG en het voorkomen of detecteren van de beschadiging daarvan;
   c. het bewaken van de zaken die zich op de terreinen van de RUG of in haar opstallen bevinden; en
   d. het voorkomen en detecteren van Incidenten.
2. Het genereren van Analysegegevens met behulp van een Camerasysteem behoeft de voorafgaande instemming van het College van Bestuur evenals het verwerken van Analysegegevens voor andere doelen dan in lid 1 van dit artikel beschreven. Deze instemming wordt gevraagd door het bestuur van de faculteit dat of de directie van de dienst die Analysegegevens wil gaan genereren en verwerken.
3. Het gebruik van Cameratoezicht, Opnamen en/of Analysegegevens voor andere doelen dan hierboven beschreven, behoeft een voorafgaand besluit van het College van Bestuur met instemming van de Universiteitsraad. Het College van Bestuur zal voor het nemen van een dergelijk besluit advies inwinnen bij de Functionaris voor de Gegevensbescherming van de RUG.
4. De RUG maakt bij haar Cameratoezicht geen gebruik van gezichtsherkenning.

[1] Zie: https://www.rug.nl/about-ug/organization/rules-and-regulations/general/20211129-algemeen-beleid-bescherming-persoonsgegevens-3-0-def.pdf

5. Wanneer de RUG audio wil vastleggen bij het maken van Opnamen ten behoeve van Cameratoezicht, dient door het verantwoordelijke faculteitsbestuur of de verantwoordelijke directie van een dienst hiervoor een DPIA te worden uitgevoerd.
6. Alvorens op basis van Opnamen en/of Analysegegevens wordt gehandeld, worden zij beoordeeld door een bevoegde medewerker van de RUG.

Artikel 4. Verdeling taken, verantwoordelijkheden en bevoegdheden

1. Het College van Bestuur van de RUG is eindverantwoordelijke voor het Cameratoezicht.
2. De Directeur Vastgoedorganisatie is belast met:
    a. Het aanschaffen en inrichten van niet-mobiele “aard- en nagelvaste” Camerasystemen ten behoeve van het Cameratoezicht dat door de RUG wordt gehouden conform een door de RUG opgesteld programma van eisen en specificaties;
    b. Het in samenspraak met de afdeling BJZ en de Privacy- & Securitycoördinator van diens organisatieeenheid laten voldoen van de apparatuur en software van het Camerasysteem aan de eisen van de AVG, dit beleid en het privacy- en informatiebeveiligingsbeleid van de RUG. Dit betekent onder meer:
        i. dat de apparatuur en software *privacy & security by design* zijn vervaardigd en ingericht en dat de toepassing van de eisen van dit beleid zo veel mogelijk technologisch wordt afgedwongen;
        ii. dat met de leveranciers van het Camerasysteem de op grond van de AVG vereiste afspraken zijn gemaakt over de verwerking en beveiliging van Opnamen en Analysegegevens;
        iii. dat Opnamen en Analysegegevens uitsluitend binnen de Europese Economische Ruimte worden verwerkt;
        iv. dat Opnamen en Analysegegevens uitsluitend zijn opgeslagen op door de Directeur Vastgoedorganisatie aangewezen systemen en niet onrechtmatig verder worden verspreid of langer worden bewaard dan noodzakelijk.
3. De Security Manager is belast met:
    a. Het adviseren van faculteitsbesturen en directies van diensten over de plaatsing, afstelling en ingebruikname van een Camerasysteem op een Locatie;
    b. Het adviseren van faculteitsbesturen en directies van diensten over de verlenging van toegang tot live Opnamen voor medewerkers van recepties, front offices en meldkamers van de faculteit of dienst;
    c. Het ondersteunen van de faculteiten en diensten bij het uitvoeren van een DPIA;
    d. Het beheren van de toegangsrechten van medewerkers van de fysieke beveiligingsorganisatie van de RUG tot gemaakte Opnamen in lijn met dit beleid;
    e. Het opstellen en publiceren van een privacyverklaring over Cameratoezicht, die de Betrokkenen volgens de eisen van de AVG

informeert over de Verwerking van Persoonsgegevens die het gevolg is van Cameratoezicht.

f. De uitoefening van de hierboven aan de Directeur Vastgoedorganisatie toegekende taken, verantwoordelijkheden en bevoegdheden in de gevallen dat het Camerasysteem mobiel is.

4. Faculteitsbesturen en Directies van diensten zijn belast met:
    a. Het nemen van een besluit over het houden van Cameratoezicht op een Locatie waarvan hun faculteit of de dienst gebruik maakt;
    b. Het gebruik van het Camerasysteem met inachtneming van de wettelijke verplichtingen uit hoofde van de AVG en andere toepasselijke wet- en regelgeving, dit beleid en het privacy- en informatiebeveiligingsbeleid van de RUG. Dit betekent onder meer:
        i. dat het gebruik van Cameratoezicht gebeurt voor de op grond van dit beleid toegestane doelen en voor het bereiken van die doelen minder ingrijpende middelen niet voldoende effectief zijn;
        ii. dat de noodzakelijkheid, subsidiariteit en proportionaliteit van het Cameratoezicht en daarmee gepaard gaande verwerkingen voorafgaand aan het nemen van een besluit daartoe wordt beoordeeld en daarna minimaal iedere drie jaar wordt geëvalueerd, waar nodig met een DPIA;
        iii. dat voor de plaatsing van een Camerasysteem advies wordt ingewonnen bij de Directeur Vastgoedorganisatie en de Security Manager;
        iv. dat voor Cameratoezicht uitsluitend Camerasystemen worden afgenomen die in het portfolio zijn opgenomen van De Directeur Vastgoedorganisatie en de Security Manager;
        v. dat uitsluitend medewerkers van de faculteit/dienst voor wie dat noodzakelijk is, toegang krijgen tot de Opnamen, Analysegegevens en Persoonsgegevens;
        vi. dat Betrokkenen worden geïnformeerd over het Cameratoezicht op de Locaties waar het faculteitsbestuur of de directie Cameratoezicht houdt;
        vii. dat minimaal iedere drie jaar wordt geëvalueerd of het Cameratoezicht nog noodzakelijk is en plaatsvindt in overeenstemming met dit beleid. Het faculteitsbestuur of de directie wijst een medewerker aan die zorgt draagt voor de uitvoering van de in het voorgaande lid genoemde verplichtingen.
5. De Directeur Vastgoedorganisatie, de Security Manager en de Faculteitsbesturen en Directies van Diensten winnen bij de uitvoering van hun taken, verantwoordelijkheden en bevoegdheden voorafgaand advies in bij de Privacy- & Securitycoördinator van hun organisatie-eenheid.
6. De onafhankelijke Functionaris voor de Gegevensbescherming van de RUG houdt toezicht op de naleving van dit beleid en brengt daarover minimaal jaarlijks verslag uit aan het College van Bestuur in diens jaarverslag bescherming persoonsgegevens. Dit verslag wordt ter informatie voorgelegd aan de universiteitsraad nadat het College van Bestuur er kennis van heeft genomen.

Artikel 5. Het plaatsen van camera's, informeren van Betrokkenen

1. Bij een besluit tot plaatsing van een Camerasysteem wordt altijd een deugdelijke afweging gemaakt tussen enerzijds de bescherming van de persoonlijke levenssfeer van de Betrokkenen en anderzijds de belangen van de RUG. De bevoegde Privacy & Security-coördinator van de faculteit of dienst adviseert of er een DPIA uitgevoerd moet worden.
2. Op Locaties waar personen ongestoord moeten kunnen zijn, zoals in toiletten, douches en kleedruimten, is Cameratoezicht te allen tijde niet toegestaan.
3. Cameratoezicht wordt alleen ingezet voor de doeleinden zoals vermeld in dit beleid, op locaties waar dit noodzakelijk is, proportioneel is en minder ingrijpende maatregelen niet (voldoende) effectief zijn.
4. De noodzaak van Cameratoezicht op een bepaalde Locatie wordt minimaal iedere drie jaar geëvalueerd. In het geval dat het Camerasysteem mobiel is, wordt de noodzaak binnen een termijn van maximaal 3 maanden heroverwogen.
5. Het Cameratoezicht wordt kenbaar gemaakt door middel van borden, stickers en/of beeldschermen bij de in- en uitgangen van de Locaties waar het Cameratoezicht wordt gehouden, alsmede in de Locaties. Deze verwijzen naar een publicatie van dit beleid en een privacyverklaring op de openbare website van de RUG. Betrokkenen worden geïnformeerd over de doeleinden van het Cameratoezicht, de omstandigheden waaronder hun Persoonsgegevens worden verwerkt en de rechten die zij hebben met betrekking tot de Verwerking van hun Persoonsgegevens.
6. Cameratoezicht is niet bedoeld om Betrokkenen tijdens het uitvoeren van hun werkzaamheden of bezoek te volgen. Bij het plaatsen van de camera's wordt daarom zoveel mogelijk voorkomen dat Betrokkenen onnodig continu in beeld zijn. Op locaties waar sprake is van verhoogde veiligheidsrisico's, zoals een relatief grote kans op agressie of diefstal, kunnen Betrokkenen continu in beeld worden gebracht als dit noodzakelijk is en minder ingrijpende maatregelen niet (voldoende) effectief zijn.
7. De Directeur Vastgoedorganisatie en de Security Manager zorgen voor een nuttige registratie van geplaatste Camerasystemen met vastlegging van de plek waar zij zijn geïnstalleerd.

Artikel 6. Bewaartermijnen

1. De Opnamen en Analysegegevens worden maximaal 14 dagen bewaard nadat ze tot stand zijn gebracht, waarna ze onomkeerbaar worden gewist, tenzij:
    a. de Opnamen en/of Analysegegevens verband houden met een Incident. In dat geval worden Beelden bewaard voor een periode van maximaal vier weken nadat het onderzoek naar of de behandeling van het Incident is afgesloten; of
    b. door een Betrokkene een verzoek is ingediend met betrekking tot de Opnamen en/of Analysegegevens. In dat geval worden de Opnamen bewaard totdat de procedure die wordt gevolgd voor de behandeling van het verzoek, is doorlopen.

Artikel 7. Toegang tot Opnamen

1. Met Cameratoezicht gemaakte Opnamen en Analysegegevens zijn enkel toegankelijk voor medewerkers van de RUG en andere personen voor wie dat noodzakelijk is met het oog op de in artikel 3 lid 1 genoemde doelen. Zij dienen instructies te krijgen ten behoeve van de zorgvuldige omgang met de Opnamen en Analysegegevens in overeenstemming met de AVG en dit beleid, voordat toegang wordt verleend.
2. Toegang tot Opnamen en Analysegegevens vindt waar mogelijk plaats binnen het Camerasysteem waarin de Opnamen en Analysegegevens zijn vastgelegd, zodat van de Opnamen en Analysegegevens geen kopieën worden gemaakt die op een andere informatiedrager worden opgeslagen.
3. Toegang tot *live* beelden en audio wordt in beginsel enkel verstrekt aan:
    a. Medewerkers van recepties, front offices en meldkamers, werkzaam op de Locaties waar en/of waaromheen de Opnamen worden gemaakt;
    b. Medewerkers van de Fysieke Beveiligingsorganisatie.
4. Toegang tot opgeslagen Opnamen en Analysegegevens wordt in beginsel enkel verstrekt aan:
    a. Medewerkers van de Fysieke Beveiligingsorganisatie;
    b. Andere medewerkers die verantwoordelijk zijn voor de fysieke beveiliging van de RUG dan wel verantwoordelijk zijn voor het beveiligen of beheren van goederen en zaken van de RUG, zulks na beoordeling en goedkeuring van de Security Manager.
5. De Security Manager registreert de verleende toegang tot opgeslagen Opnamen en Analysegegevens. De Security Manager controleert minimaal jaarlijks de toegangsrechten tot de Camerasystemen om onbevoegde toegang zoveel mogelijk uit te sluiten.

Artikel 8. Heimelijk Cameratoezicht

1. Alleen in bijzondere omstandigheden kan op Locaties van de RUG Heimelijk Cameratoezicht worden ingezet. Er moet sprake zijn van een redelijk vermoeden van strafbaar of frauduleus handelen van de persoon of personen op wie het Heimelijk Cameratoezicht is gericht.
2. Het besluit tot het houden van Heimelijk Cameratoezicht wordt op basis van een door het verantwoordelijke faculteitsbestuur of de verantwoordelijke directie van een dienst opgestelde onderbouwing, met advies van het Hoofd Bestuurlijke en Juridische Zaken, genomen door het College van Bestuur.
3. Het Hoofd BJZ is verantwoordelijk voor het uitvoeren van een overkoepelend DPIA op Heimelijk Cameratoezicht. De universiteitsraad ontvangt ter informatie een afschrift van dit DPIA.
4. Heimelijk Cameratoezicht is altijd tijdelijk gedurende een door het bevoegde faculteitsbestuur of directie van een dienst voorgestelde periode. Deze periode is maximaal 3 maanden.

5. Heimelijk Cameratoezicht is toegestaan op duidelijk afgebakende Locaties en slechts gericht op het aantonen van handelen als bedoeld in lid 1. Universiteitsbreed of faculteitsbreed Heimelijk Cameratoezicht is niet toegestaan.
6. Heimelijk Cameratoezicht kan enkel worden ingezet als 'laatste middel', nadat is gebleken dat andere middelen niet (voldoende) effectief zijn. Heimelijk Cameratoezicht wordt uitgevoerd door onafhankelijke personen, die zo nodig niet bij de RUG werkzaam zijn.
7. De RUG zal de Betrokkene(n) achteraf informeren over de inzet van Heimelijk Cameratoezicht zodra de inzet hiervan niet meer noodzakelijk is om doeleinden zoals vermeld in artikel 8 lid 1 te bereiken.
8. De Opnamen gemaakt met Heimelijk Cameratoezicht zijn uitsluitend toegankelijk voor de leden van het bevoegde faculteitsbestuur of de bevoegde dienstdirectie, het Hoofd Bestuurlijke en Juridische Zaken, de Functionaris voor de Gegevensbescherming en de leden van het College van Bestuur. Dit in afwijking van artikel 7 lid 3 en 4 van dit beleid.
9. De in artikel 6 genoemde bewaartermijnen zijn ook van toepassing op Opnamen die gemaakt zijn met Heimelijk Cameratoezicht.

Artikel 9. Inzage en verstrekking van Opnamen aan derden

1. Inzage in- en verstrekking van de Opnamen en/of Analysegegevens aan derden vindt alleen plaats:
   a. op vordering van de politie of het Openbaar Ministerie;
   b. bij aangifte van (een vermoeden van) een strafbaar feit; of
   c. in andere gevallen wanneer dit verenigbaar is met doeleinden zoals vermeld in dit beleid en de wet hiervoor een grondslag biedt.
2. Verzoeken om inzage in en verstrekking van Opnamen en/of Analysegegevens dienen te worden ingediend bij het Hoofd Bestuurlijke en Juridische Zaken van de RUG. Het Hoofd Bestuurlijke en Juridische Zaken toetst of de vordering van de politie of het Openbaar Ministerie voldoende grondslag biedt voor de gevraagde inzage en/of uitgifte. Het Hoofd Bestuurlijke en Juridische Zaken heeft het mandaat om namens het College van Bestuur te besluiten over een verzoek tot inzage of verstrekking.
3. Feitelijke uitvoering van het verzoek gebeurt door de Security Manager. Eenieder die de Opnamen en/of Analysegegevens mag inzien of daarvan een kopie ontvangt, dient zich vooraf bij de Security Manager te legitimeren. De Security Manager registreert het verzoek en besluit tot verstrekking.

Artikel 10. Rechten van Betrokkenen

1. Een Betrokkene heeft recht op inzage in de Persoonsgegevens die zijn vastgelegd in de Opnamen en Analysegegevens. De RUG heeft het recht de Betrokkene te vragen toe te lichten waar en wanneer volgens de Betrokkene Opnamen van hem of haar zijn gemaakt, alvorens zij start met de behandeling van een verzoek om inzage.

2. De RUG kan inzage weigeren, bijvoorbeeld als dat noodzakelijk is in het belang van voorkoming, opsporing en vervolging van strafbare feiten of ter bescherming van rechten en vrijheden van anderen.
3. Een Betrokkene heeft recht op verwijdering of afscherming van Persoonsgegevens die hem of haar betreffen, voor zover die Persoonsgegevens onrechtmatig verwerkt worden of de Persoonsgegevens niet (meer) relevant zijn voor het doel waarvoor zij zijn verzameld.
4. Een Betrokkene heeft het recht bezwaar te maken tegen het gebruik van zijn of haar Persoonsgegevens door de RUG. De RUG maakt een afweging tussen het bezwaar van de Betrokkene en het belang van de organisatie. Als het bezwaar van de Betrokkene gegrond is, beëindigt de RUG de betreffende Verwerking.
5. De verzoeken als bedoeld in lid 1, lid 3 en lid 4 kunnen worden gericht aan het centraal loket Privacy via privacy@rug.nl.

Artikel 11. Klachten

1. Een Betrokkene kan te allen tijde contact opnemen met de Functionaris voor de Gegevensbescherming van de RUG over alle aangelegenheden die verband houden met de verwerking van zijn of haar Persoonsgegevens. Dit kan per e-mail via fg@rug.nl.
2. Klachten over de toepassing van het Cameratoezicht en de uitvoering van dit beleid, kunnen schriftelijk worden ingediend bij het College van Bestuur volgens de procedure van de algemene klachtenregeling van de RUG.[2]
3. De Betrokkene kan te allen tijde een klacht indienen bij de Autoriteit Persoonsgegevens[3] over de verwerking van Persoonsgegevens door de RUG.

Artikel 12. Slotbepalingen

1. Dit beleid is, na instemming van de universiteitsraad, vastgesteld door het College van Bestuur op 23 mei 2025 en vanaf dat moment van toepassing.
2. Dit beleid vervangt de Regeling Cameratoezicht Rijksuniversiteit Groningen, laatstelijk vastgesteld op 13 juli 2015.
3. Het beheer van dit beleid is belegd bij de Chief Privacy Officer van de RUG.
4. In gevallen waarin dit beleid niet voorziet, beslist het College van Bestuur met inachtneming van de toepasselijke rechten en bevoegdheden van de Universiteitsraad.
5. Dit beleid wordt uiterlijk drie jaar na de dag waarop het van toepassing is geworden geëvalueerd.

[2] Zie: https://www.rug.nl/about-ug/organization/rules-and-regulations/vertrouwelijkheid-klachten-bezwaar-beroep/algemene-klachtenregeling
[3] Zie de website van de AP: https://www.autoriteitpersoonsgegevens.nl/een-tip-of-klacht-indienen-bij-de-ap#het-meldformulier.