Bijlage 1: Relevante wettelijke bepalingen

Artikel 5.1 Uitzonderingen

1. Het openbaar maken van informatie ingevolge deze wet blijft achterwege voor zover dit:
   a) de eenheid van de Kroon in gevaar zou kunnen brengen;
   b) de veiligheid van de Staat zou kunnen schaden;
   c) bedrijfs- en fabricagegegevens betreft die door natuurlijke personen of rechtspersonen vertrouwelijk aan de overheid zijn meegedeeld;
   d) persoonsgegevens betreft als bedoeld in paragraaf 3.1 onderscheidenlijk paragraaf 3.2 van de Uitvoeringswet Algemene verordening gegevensbescherming, tenzij de betrokkene uitdrukkelijk toestemming heeft gegeven voor de openbaarmaking van deze persoonsgegevens of deze persoonsgegevens kennelijk door de betrokkene openbaar zijn gemaakt;
   e) nummers betreft die dienen ter identificatie van personen die bij wet of algemene maatregel van bestuur zijn voorgeschreven als bedoeld in artikel 46 van de Uitvoeringswet Algemene verordening gegevensbescherming, tenzij de verstrekking kennelijk geen inbreuk op de levenssfeer maakt.

2. Het openbaar maken van informatie blijft eveneens achterwege voor zover het belang daarvan niet opweegt tegen de volgende belangen:
   a) de betrekkingen van Nederland met andere landen en staten en met internationale organisaties;
   b) de economische of financiële belangen van de Staat, andere publiekrechtelijke lichamen of bestuursorganen, in geval van milieu-informatie slechts voor zover de informatie betrekking heeft op handelingen met een vertrouwelijk karakter;
   c) de opsporing en vervolging van strafbare feiten;
   d) de inspectie, controle en toezicht door bestuursorganen;
   e) de eerbiediging van de persoonlijke levenssfeer;
   f) de bescherming van andere dan in het eerste lid, onderdeel c, genoemde concurrentiegevoelige bedrijfs- en fabricagegegevens;
   g) de bescherming van het milieu waarop deze informatie betrekking heeft;
   h) de beveiliging van personen en bedrijven en het voorkomen van sabotage;
   i) het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen.

3. Indien een verzoek tot openbaarmaking op een van de in het tweede lid genoemde gronden wordt afgewezen, bevat het besluit hiervoor een uitdrukkelijke motivering.

4. Openbaarmaking kan tijdelijk achterwege blijven, indien het belang van de geadresseerde van de informatie om als eerste kennis te nemen van de informatie dit kennelijk vereist. Het bestuursorgaan doet mededeling aan de verzoeker van de termijn waarbinnen de openbaarmaking alsnog zal geschieden.

5. In uitzonderlijke gevallen kan openbaarmaking van andere informatie dan milieu-informatie voorts achterwege blijven indien openbaarmaking onevenredige benadeling toebrengt aan een ander belang dan genoemd in het eerste of tweede lid en het algemeen belang van openbaarheid niet tegen deze benadeling opweegt. Het bestuursorgaan baseert een beslissing tot achterwege laten van de openbaarmaking van enige informatie op deze grond ten aanzien van dezelfde informatie niet tevens op een van de in het eerste of tweede lid genoemde gronden.

6. Het openbaar maken van informatie blijft in afwijking van het eerste lid, onderdeel c, in geval van milieu-informatie eveneens achterwege voor zover daardoor het in het eerste

lid, onderdeel c, genoemde belang ernstig geschaad wordt en het algemeen belang van openbaarheid van informatie niet opweegt tegen deze schade.
7. Het eerste en tweede lid zijn niet van toepassing op milieu-informatie die betrekking heeft op emissies in het milieu.

Bijlage 2: inventarislijst

Nummer	Document	Beoordeling	Grond
1	Factsheet: Logging Verwerking	Openbaar maken	
2	Memo nadere afbakening loggingsverplichting	Gedeeltelijk openbaar maken	5.1.2e
3	Informatiebeveiligingsbeleid 2023	Gedeeltelijk openbaar maken	Buiten reikwijdte verzoek

Bijlage 3: Documenten

OPENBAAR MINISTERIE

Factsheet: Logging Verwerking Persoonsgegevens

Versie: 10 januari 2022

Waarom

De privacywet- en regelgeving op Europees niveau is vastgelegd in de GDPR (General Data Protection Regulation) en (voor justitie) in de Richtlijn Gegevensbescherming Opsporing en Vervolging. In Nederland is de GDPR in de wetgeving opgenomen (juridische vertaling) in de vorm van de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). De Richtlijn is in Nederland vertaald naar de Wet Politiegegevens (WPG) en de Wet Justitiële en Strafvorderlijke Gegevens (Wjsg). Het "bijhouden van logbestanden van verwerkingen van persoonsgegevens" is een verplichting onder de Richtlijn, zoals beschreven in Artikel 25.

Logging is een geautomatiseerde registratie van gegevens, bedoeld om bij te houden welke gebeurtenissen en handelingen binnen een systeem hebben plaatsgevonden. Door middel van logging kan bijvoorbeeld worden gecontroleerd of er een goede reden was voor een medewerker om bepaalde gegevens in te zien (rechtmatigheid).

Het OM moet voldoen aan de logverplichting om verantwoording over het gebruik van persoonsgegevens binnen OM te kunnen afleggen. Specifieke doelen van de logging zijn:

- Controleren en aantonen van de rechtmatigheid van de verwerking;
- Faciliteren van interne controles;
- Waarborging van de beveiliging en integriteit van persoonsgegevens;
- Gebruik voor strafrechtelijke procedures gerelateerd aan inbreuken op voorgaande aspecten (bijv. inzake ambtelijke corruptie).

Wat wordt gelogd

Van de volgende soorten verwerkingen van persoonsgegevens en gegevens over rechtspersonen worden loggegevens bijgehouden:

- verzameling van gegevens
- raadpleging van gegevens
- verstrekking van gegevens
- wijziging van gegevens
- vernietiging van gegevens

Met betrekking tot de verwerking raadpleging worden de volgende gegevens gelogd:

Gegeven	Toelichting
Datum/tijd verwerking	Dit is de datum en het tijdstip waarop de verwerking heeft plaatsgevonden.
Gebruikers ID	Unieke identificatie in de applicatie van de gebruiker die de gegevens verwerkt heeft.
Soort identificatie gegevensverwerker	Aanvullende informatie ten behoeve van de herleidbaarheid van het gebruikers ID.
Dossier ID / Zaak ID / Parketnummer	Unieke identificatie van de zaak/dossier.
Type zaak	Betreft veelal 'Strafzaak', maar indien er geen strafzaak is, kan dit afwijken.

Welke applicaties

Voor de volgende applicaties is Logging Verwerking Persoonsgegevens geïmplementeerd:

- Module Onderzoeken
- HELIX
- ED NIAS
- GPS
- NIAS
- LZOZ

Wie heeft toegang tot loggegevens

De logging van de verwerking van persoonsgegevens heeft betrekking op alle gebruikers van bovengenoemde verwerkingen en applicaties en betreft een **continue activiteit**.

Toegang tot de loggegevens is strikt beperkt tot Functioneel Beheer IVOM in opdracht van geautoriseerde functionarissen die belast zijn met het analyseren van de loggegevens. De loggegevens worden bewaard conform de bewaartermijnen zoals beschreven in de Wjsg, het Wetboek van Strafvordering en de Archiefwet.

Meer weten?

Voor vragen over logging kun je terecht bij de privacy en/of security functionaris op jouw locatie. Meer informatie over logging is ook te vinden op de pagina Personeel op ZoOM Hier vind je het document "Wegwijzer gedragsregels".

2. Informatiebeveiliging

Het is belangrijk om zorgvuldig om te gaan met informatie van het werk en bewust te zijn van eventuele informatiebeveiligingsrisico's. Bijvoorbeeld, door het - al dan niet bewust - lekken van (gevoelige of vertrouwelijke) informatie wordt het vertrouwen in de overheid geschaad. Bevoegdheden en informatie gebruik je alleen voor het doel waarvoor je ze hebt verkregen. Je deelt vertrouwelijke informatie niet met anderen. Meer informatie vind je op deze pagina, of in paragraaf 3.2 en 4.3 van de Gedragscode Integriteit Rijksambtenaren (GIR).

In dit document is een verwijzing opgenomen naar het document "Gedragsregeling voor de digitale werkomgeving" met hierin richtlijnen over logging en monitoring.

Let op! Je kunt dit document openen door in paragraaf 2. "Informatiebeveiliging" van de Wegwijzer gedragsregels (zie bovenstaand voorbeeld), te klikken op "deze pagina" en dan naar pagina 15, paragraaf "Logging, monitoring en controle".

OPENBAAR MINISTERIE

Parket-Generaal

Aan Rinus Otte en [redacted]

Van [redacted]

Datum 14-03-2023

Onderdeel WBOM/R&I

Onderwerp Nadere afbakening loggingsverplichting

Memo

1 Aanleiding

Op grond van artikel 25 EU-Richtlijn gegevensbescherming opsporing en vervolging (hierna Richtlijn) moeten de lidstaten erin voorzien dat er logbestanden worden bijgehouden van een aantal verwerkingen van strafrechtelijke persoonsgegevens. Deze verwerkingen moeten zijn gedaan in systemen voor geautomatiseerde verwerking. De Nederlandse wetgever heeft deze bepaling geïmplementeerd door het College van procureurs-generaal – de verwerkingsverantwoordelijke voor de verwerking van strafrechtelijke persoonsgegevens door het openbaar ministerie – te verplichten zorg te dragen voor de logging van strafvorderlijke gegevens en tenuitvoerleggingsgegevens (artikel 26e i.c.m. 39r en 51d Wjsg). Artikel 26e Wjsg komt – na inwerkingtreding – te luiden (waarbij strafvorderlijke gegevens en tenuitvoerleggingsgegevens moeten worden gelezen in plaats van justitiële gegevens):

> 1.De verwerkingsverantwoordelijke en de verwerker dragen zorg voor de vastlegging langs elektronische weg (logging) van ten minste de volgende verwerkingen van justitiële gegevens in geautomatiseerde systemen: het verzamelen, wijzigen, raadplegen, verstrekken onder meer in de vorm van doorgiften, combineren en vernietigen van justitiële gegevens.
> 2.De vastgelegde gegevens, bedoeld in het eerste lid, worden uitsluitend gebruikt voor de controle van de rechtmatigheid van de gegevensverwerking, voor interne controles, ter waarborging van de integriteit en de beveiliging van de justitiële gegevens en voor strafrechtelijke procedures.

Artikel 26e Wjsg is nog niet in werking getreden. Een inwerkingtredingsdatum is ook nog niet gegeven. De Europese wetgever heeft in artikel 63 Richtlijn toegestaan dat de implementatie van de loggingsverplichting wordt uitgesteld tot 6 mei 2023. Verder uitstel is in uitzonderlijke omstandigheden zelfs mogelijk tot 6 mei 2026, maar dan alleen onder de voorwaarde dat de werking van het gebruikte systeem voor geautomatiseerde verwerking anders ernstig in het gedrang zou komen. Ook is de voorwaarde dat de betrokken lidstaat de Commissie in kennis stelt van de redenen voor die ernstige moeilijkheden en voor de nader bepaalde termijn waarbinnen de lidstaat het genoemde systeem voor geautomatiseerde verwerking met artikel 25, lid 1, in overeenstemming brengt.

Het College moet als verwerkingsverantwoordelijke inschatten in hoeverre het openbaar ministerie op dit moment al voldoet aan de loggingsverplichting, of daar binnenkort aan kan voldoen. Deze informatie kan vervolgens worden doorgegeven aan het ministerie van Justitie en Veiligheid, zodat het ministerie hier rekening mee kan houden bij het bepalen van de inwerkingtredingsdatum van artikel 26e Wjsg te kunnen bepalen. Voordat het College kan vaststellen of het openbaar ministerie zich houdt aan de (toekomstige) loggingsverplichting, is het van belang te bepalen wat de loggingsverplichting inhoudt, in welke gevallen de loggingsverplichting van toepassing is, en hoe de loggingsverplichting moet worden afgebakend.

Binnen het openbaar ministerie zijn al de nodige beleidsdocumenten verschenen die betrekking hebben op de afbakening en invulling van de loggingsverplichting. Met name kan worden gedacht aan het document 'Baseline gegevensbescherming OM, loggingsverplichting' (versie 19 september 2022) en aan 'Business Requirements IT-systemen' (versie 1.1 8 januari 2019), par. 2.5 Loggen verwerkingen persoonsgegevens.

Deze memo heeft als doel een nadere afbakening te geven van de loggingsverplichting in aanvulling op de bovengenoemde documenten. In deze memo worden uitsluitend de punten besproken waarover onduidelijkheden of vragen bestaan. Begonnen wordt met het doel van de loggingsverplichting (par. 2). Daarna wordt ingegaan op de afbakening van de loggingsverplichting (par. 3), de inhoud van de loggingsverplichting (par. 4), de bewaartermijnen (par. 5), inzage in de logbestanden (par. 6) en het gebruik van de logbestanden (par. 7).

2 Doel loggingsverplichting

De reikwijdte van de loggingsverplichting moet worden vastgesteld in het licht van het doel van de loggingsverplichting. Het directe doel dat met de loggingsverplichting wordt nagestreefd, kan worden gevonden in wat met de logbestanden kan worden gedaan. De logbestanden (of in de terminologie van de Wjsg 'de vastgelegde gegevens) kunnen volgens artikel 25 lid 2 Richtlijn en artikel 26e lid 2 Wjsg worden gebruikt om 'te controleren of de verwerking rechtmatig is, voor interne controles, ter waarborging van de integriteit en de beveiliging van de persoonsgegevens en voor strafrechtelijke procedures'. De logbestanden mogen uitsluitend voor deze doelen worden gebruikt. Er kan zelfs sprake zijn van bovenmatige en daarmee onrechtmatige verwerking van persoonsgegevens door logbestanden aan te maken voor doelen waarvoor ze niet mogen worden gebruikt. De gebruiksdoelen geven dus een kader voor in welke gevallen de logbestanden moeten worden gemaakt.

Het onderliggende doel dat met de loggingsverplichting wordt nagestreefd, is het doel dat met de gegevensbeschermingsregels in het algemeen wordt nagestreefd. Mensen hebben het recht op bescherming van hun privacy en

het recht op bescherming van hun persoonsgegevens. Voor de duidelijkheid: dit zijn geen absoluut rechten, maar een inbreuk op deze rechten moet wel kunnen worden gerechtvaardigd. Als het gaat om strafrechtelijke persoonsgegevens gaat het om de rechten van personen die betrokken zijn bij strafzaken: verdachten, slachtoffers, getuigen, et cetera. Van het openbaar ministerie wordt verwacht dat het strafrechtelijke persoonsgegevens op behoorlijke, rechtmatige, doelgebonden, proportionele en subsidiaire wijze verwerkt. Logging kan eraan bijdragen dat de strafrechtelijke persoonsgegevens juist zijn en dat er op rechtmatige wijze met deze gegevens wordt omgegaan. Dit draagt er op zijn beurt weer aan bij dat het openbaar ministerie en de strafrechter rechtvaardige en rechtmatige beslissingen kunnen nemen in een strafzaak – wat het einddoel zou moeten zijn van elke strafzaak.

De art. 29 Data Protection Working Party (hierna WP29) heeft in zijn commentaar op de Richtlijn zich ook uitgelaten over het doel van de loggingsverplichting.[1] Volgens de WP29 moeten de logs het mogelijk maken "to trace the users' activity to spot abusive use." Centraal staat in deze benadering het voorkomen van misbruik. De WP29 wijst erop dat er vervolgens ook consequenties zouden moeten worden verbonden aan de vaststelling dat gegevens zijn verwerkt zonder dat de persoon die dat doet daartoe gerechtigd is.

Duidelijk is dat het loggen van verwerkingen geen op zichzelf staand doel is. Het loggen van verwerkingen is een middel om te controleren of de gegevens juist zijn en de verwerkingen rechtmatig – een middel om misbruik van gegevens te voorkomen. Dit blijkt ook duidelijk uit de preambule van de Richtlijn (overweging 57): 'De logbestanden dienen uitsluitend te worden gebruikt om te controleren of de gegevensverwerking rechtmatig is, om interne controle uit te oefenen, om de integriteit en de beveiliging van de gegevens te garanderen en om strafrechtelijke procedures te waarborgen. Interne controle dient interne tuchtprocedures van bevoegde autoriteiten te omvatten.' Deze overweging is vrijwel letterlijk terug te vinden in artikel 25 lid 2 Richtlijn en (zoals hierboven al aangehaald) artikel 26e lid 2 Wjsg. De laatste zin over de interne tuchtprocedures staat niet in de bepalingen, maar maakt nog duidelijker dat de logging een middel is om onrechtmatige verwerkingen tegen te gaan, omdat hieraan ook consequenties behoren te worden verbonden.

Naast het loggen van de verwerkingen zijn er ook andere manieren waarop kan worden gecontroleerd dat gegevens juist zijn en verwerkingen rechtmatig. Uit het feit dat het loggen van verwerking bijdraagt aan het verwezenlijken van deze doelen, kan niet de conclusie worden getrokken dat de logging verplicht is om deze doelen te bereiken. In die denkwijze worden doel en middel onterecht gelijk gesteld. Met andere woorden, uit het feit dat een logbestand kan worden gebruikt om de rechtmatigheid de gegevensverwerking te controleren, volgt geen verplichting om telkens als het wenselijk is de

[1] Article 29 Data Protection Working Party, 'Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)', 29 november 2017, p. 26.

rechtmatigheid van de verwerking van persoonsgegevens te controleren – dat is immers in beginsel wenselijk bij elke verwerking – deze verwerking te loggen.

Worden gegevens onrechtmatig verwerkt dan is er sprake van misbruik van gegevens. Maar dit misbruik van persoonsgegevens en de potentiele schade als gevolg daarvan kent verschillende gradaties van ernst. Ernstig is het als gebruik van onjuiste persoonsgegevens leidt tot onjuiste en onrechtvaardige uitspraken. Ook ernstig is het als misbruik van persoonsgegevens invloed heeft op de veiligheid of het welzijn van betrokken personen, bijvoorbeeld omdat persoonsgegevens van slachtoffers terechtkomen bij de verdachte of persoonsgegevens van de verdachte bij de media. Niet alle onrechtmatige verwerkingen van persoonsgegevens hebben dergelijke ernstige consequenties. Net zomin als de loggingsverplichting een doel op zichzelf is, mag de controle of de verwerking rechtmatig is of het waarborgen van de integriteit en de beveiliging van de persoonsgegevens een doel op zichzelf worden. Ook bij de uitleg van de loggingsverplichting moeten de gevolgen voor de uitoefening van de wettelijke taken door het openbaar ministerie in acht worden genomen. Het streven naar eliminatie van elk misbruik – op zichzelf al onmogelijk – kent als risico dat het openbaar ministerie wordt belemmert bij de uitoefening van wettelijke taken en kan leiden tot een bovenmatig beslag op de beschikbare schaarse middelen.

3 Afbakening loggingsverplichting

3.1 Voorwaarden loggingsverplichting

Uit de tekst van artikel 26e lid 1 Wjsg staan drie voorwaarden waaraan moet zijn voldaan voordat er sprake is van een loggingsverplichting. De bepaling luidt (voor zover relevant): "De verwerkingsverantwoordelijke en de verwerker dragen zorg voor de vastlegging langs elektronische weg (logging) van ten minste de volgende verwerkingen van justitiële gegevens in geautomatiseerde systemen". Hieruit volgt dat er alleen een loggingsverplichting bestaat als er sprake is van:
1) dat er strafrechtelijke persoonsgegevens worden verwerkt;
2) de verwerking plaatsvindt in geautomatiseerde systemen;
3) de verwerkingsverantwoordelijke het beheer heeft over de geautomatiseerde systemen.

3.2 Verwerking strafrechtelijke persoonsgegevens

De loggingsverplichting is gezien artikel 26e, 39r en 51d van toepassing op onder meer justitiële gegevens, strafvorderlijke gegevens en tenuitvoerleggingsgegevens. In het strafvorderlijk kader gegevensverwerking door het openbaar ministerie is uiteengezet waarom het de voorkeur verdient om in plaats van deze termen de Richtlijnconforme term strafrechtelijke persoonsgegevens te gebruiken. Met de term strafrechtelijke persoonsgegevens wordt bedoeld persoonsgegevens die mogelijk verband houden met het voorkomen van en het onderzoek naar strafbare feiten, de opsporing, vervolging en berechting van verdachten en tenuitvoerlegging van straffen.

De loggingsverplichting geldt niet voor de verwerking van niet-

strafrechtelijke persoonsgegevens. Ook niet als deze gegevens worden verwerkt onder verantwoordelijkheid van het College. In de AVG staat geen loggingsverplichting. Mogelijk kan het soms wenselijk zijn om in het kader van de beveiliging en integriteit van gegevens te loggen welke verwerkingen zijn uitgevoerd. Deze wens moet echter los worden gezien van de loggingsverplichting van artikel 25 Richtlijn en artikel 26e Wjsg.

> *In de Baseline wordt een onderscheid gemaakt tussen logging voor controledoelen (waarmee de loggingsverplichting uit de Richtlijn lijkt te worden bedoeld) en logging voor beveiligingsdoelen (waarmee logging om andere redenen lijkt te worden bedoeld). In de Baseline zou nog kunnen worden verduidelijkt dat er onder de AVG geen verplichting is tot logging voor gegevensbeschermingsdoelen.*

De loggingsverplichting geldt ook niet als er geen persoonsgegevens worden verwerkt. Dit is het geval bij de verwerking van geanonimiseerde gegevens. Geanonimiseerde gegevens zijn gegevens die niet meer kunnen worden herleid tot een persoon. Ook bij de verwerking van gepseudonimiseerde persoonsgegevens hoeft er geen sprake te zijn van een verwerking van persoonsgegevens. Bij pseudonimisering worden de persoonsgegevens versleuteld, waardoor de gegevens niet meer aan een persoon kunnen worden gekoppeld zonder beschikking te hebben over de sleutel. Het Hof van Justitie heeft overwogen dat er geen sprake is van persoonsgegevens als het koppelen van de gegevens aan een persoon "bij de wet verboden wordt of in de praktijk ondoenlijk is, bijvoorbeeld omdat zij – gelet op de vereiste tijd, kosten en mankracht – een excessieve inspanning vergt, zodat het gevaar voor identificatie in werkelijkheid onbeduidend lijkt."[2] Hieruit kan worden afgeleid dat zolang degene die de verwerking uitvoert geen toegang heeft en kan krijgen tot de gegevens die nodig zijn om de gepseudonimiseerde persoonsgegevens weer terug te herleiden tot de persoon die het betreft, er geen sprake is van een verwerking van persoonsgegevens. **Kortom: bij systemen waar gegevens worden verwerkt die door de gebruiker niet kunnen worden gekoppeld aan een persoon, is er (voor de verwerking door deze gebruiker) geen loggingsverplichting.** Dit is anders voor degene die wel toegang heeft tot de sleutel – diegene die gepseudonimiseerde gegevens kan ontsleutelen verwerkt wel persoonsgegevens, en bij die verwerking kan er wel een loggingsverplichting bestaan.

Uit de Richtlijn volgt dat er ook geen persoonsgegeven worden verwerkt als er gegevens worden verwerkt van rechtspersonen. **De logging van de verwerkingen van de gegevens van rechtspersonen is gezien de Richtlijn niet verplicht.** De Richtlijn eist echter ook niet dat onderscheid wordt gemaakt tussen natuurlijke personen en rechtspersonen – zeker niet als dit tot aanvullende problemen leidt. De logging van de gegevens van rechtspersonen is ook niet verboden. Zogezien is het geen probleem dat in de definitiebepalingen van de

[2] Hof van Justitie 19 oktober 2016, C-582/14 (Breyer t. Duitsland), onder 46.

Wjsg de gegevens over rechtspersonen worden gelijkgesteld met persoonsgegevens van natuurlijke personen.

3.3 Verwerkingen in geautomatiseerde systemen

De loggingsverplichting geldt voor verwerkingen in systemen voor geautomatiseerde verwerking (Richtlijn) of geautomatiseerde systemen (Wjsg). Aangenomen mag worden dat hiermee hetzelfde wordt bedoeld. De Richtlijn is in zijn geheel van toepassing op geheel of gedeeltelijke geautomatiseerde verwerking en niet-geautomatiseerde verwerking van persoonsgegevens (artikel 2 lid 2 Richtlijn). Een definitie van de begrippen 'geautomatiseerde verwerking' en 'systeem voor geautomatiseerde verwerking' wordt niet gegeven. Ook in de AVG, waarin dezelfde begrippen worden gebruikt, ontbreekt een definitie. Bij gebreke aan een wettelijke definitie, moeten er andere argumenten worden gezocht die kunnen helpen bij de uitleg van het begrip 'systeem voor geautomatiseerde verwerking'. Uiteindelijk heeft de verwerkingsverantwoordelijke de plicht en de ruimte om te bepalen hoe het begrip systeem voor geautomatiseerde verwerking moet worden uitgelegd.

Rechtshistorisch

Het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens van de Raad van Europa uit 1981 bevat een definitie van 'geautomatiseerde verwerking': *"automatic processing" includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination*. Deze definitie houdt niets anders in dan dat geautomatiseerde verwerking betekent: verwerking waarbij een digitaal apparaat wordt gebruikt.

Na het Verdrag uit 1981 is het begrip 'geautomatiseerde verwerking' niet opnieuw gedefinieerd in internationale verdragen. Wel wordt het begrip vaker gebruikt in internationale verdragen, waaronder de voorloper van de AVG – Richtlijn 95/46/EG. Wel bevat overweging 10 uit preambule bij deze de Richtlijn de overweging dat doel van de Richtlijn is om beginselen uit 1981 'verduidelijken en versterken'. Hiermee wordt niet expliciet aangegeven dat ook de definities uit de Richtlijn van 1981 worden overgenomen. In de memorie van de Wet bescherming persoonsgegevens – waarmee de Richtlijn 95/46/EG in Nederland werd geimplementeerd – wordt wel gesteld dat 'zodra informatie digitaal is vastgelegd is er in ieder geval sprake van geautomatiseerde verwerking van gegevens'.[3]

Tegen het gebruik van deze interpretatiemethode pleit dat anno 2023 de definitie van 'geautomatiseerde systemen' verouderd is. In de definitie zijn de vele en omvangrijke ontwikkelingen op het gebied van digitalisering niet verwerkt – van de introductie van personal computers tot de uitrol van het internet, de opkomst van smartphones en de razendsnelle ontwikkeling van algoritmes en

[3] Kamerstukken II 1997-98, 25892, nr. 3 (MvT), p. 71.

kunstmatige intelligentie. Tegenwoordig vindt vrijwel elke verwerking van persoonsgegevens plaats met behulp van een digitaal apparaat – of dat nu een personal computer, laptop, tablet of smartphone is. Zonder actualisatie is het onredelijk om de verouderde definitie te gebruiken.

Wetssystematisch
In artikel 2 lid 2 Richtlijn wordt zoals gezegd onderscheid gemaakt tussen geheel en gedeeltelijk geautomatiseerde en niet-geautomatiseerde verwerking. Dit onderscheid heeft weinig tot geen betekenis als geautomatiseerde verwerking hetzelfde betekent als verwerking met behulp van een digitaal apparaat. Dat de Europese wetgever een substantiëler onderscheid voor ogen had, kan worden afgeleid uit het feit dat in de Richtlijn aanvullende eisen worden gesteld aan de geautomatiseerde verwerking van gegevens (zie artikel 29 lid 2 Richtlijn). Hieruit kan worden afgeleid dat het begrip 'geautomatiseerde verwerking' tegenwoordig beperkter moet worden geïnterpreteerd. Het was immers niet de bedoeling van de wetgever om deze extra eisen van toepassing te laten zijn op elke verwerking van strafrechtelijke persoonsgegevens, anders waren de verplichtingen niet als aanvulling gesteld bij de verplichtingen die gelden voor elke verwerkingen van persoonsgegevens.

Naast de loggingsverplichting (art. 25) en de aanvullende eisen aan geautomatiseerde verwerking (art. 29) is artikel 11 Richtlijn de bepaling waarin geautomatiseerde verwerking wordt genoemd. Die bepaling ziet op het begrenzen van geautomatiseerde besluitvorming. Ook dit impliceert dat geautomatiseerde verwerking een zwaarder begrip is, dan uitsluitend het gebruik van digitale apparaten.

Wetsgeschiedenis
In de preambule van de Richtlijn wordt handmatige verwerking gebruikt als synoniem voor niet-geautomatiseerde verwerking (preambule onder 18). Aangenomen moet worden dat hieronder ook de handmatige invoer van gegevens in computersystemen wordt verstaan, want handgeschreven documenten die betrekking hebben op de opsporing en vervolging zijn tegenwoordig een zeldzaamheid. Dit kan ook worden afgeleid uit de preambule onder 56, waarin staat dat er verwerking in systemen voor niet-geautomatiseerde verwerking mogelijk is. Wederom valt hierbij tegenwoordig vrijwel alleen te denken aan computersystemen, omdat handmatige analoge systemen die worden gebruikt bij willekeurig welke verwerking dan ook slecht denkbaar zijn.

Synthese
Uit de wetssystematiek en wetsgeschiedenis kan worden afgeleid dat geautomatiseerde verwerking niet hetzelfde is als de verwerking van persoonsgegevens met behulp van digitale apparaten. **Een redelijke invulling van dit beperktere begrip is dat tegenwoordig met geautomatiseerde verwerking wordt bedoeld: de grootschalige verwerking van persoonsgegevens.** Bij grootschalige verwerking is het stellen van aanvullende

eisen aan de verwerking te rechtvaardigen, en bovendien kan alleen grootschalige verwerking een potentiele grondslag bieden voor geautomatiseerde besluitvorming. **Bij systemen voor geautomatiseerde verwerking kan vervolgens worden gedacht aan: programma's waarin grootschalig persoonsgegevens worden vastgelegd, gewijzigd en gecombineerd.**

Voor wat betreft het openbaar ministerie kan bij systemen voor geautomatiseerde verwerking worden gedacht aan zaakssystemen als GPS, Compas, NIAS, LZOZ en de module Onderzoeken. Ook kan worden gedacht aan systemen waarin andere persoonsgegevens worden verzameld, zoals Helix, waarin DNA-gegevens zijn opgeslagen. Wat in beginsel niet als geautomatiseerde systemen hoeft te worden aangemerkt is de verwerking van gegevens met behulp van kantoorautomatiseringsprogramma's als Word, Excel en Outlook. Ook niet als deze programma's worden gebruikt voor het geautomatiseerd ordenen of selecteren van de gegevens.

Nadere opmerkingen over grootschaligheid

Breed gebruik van een systeem binnen het openbaar ministerie is niet noodzakelijk om als systeem voor geautomatiseerde verwerking te worden aangemerkt. Het is denkbaar dat bepaalde programma's slechts binnen delen van het openbaar ministerie worden gebruikt, maar binnen dat deel wel de basis vormen voor gezamenlijke en grootschalige verwerking van persoonsgegevens. Dan moeten deze programma's ook worden aangemerkt als systemen voor geautomatiseerde verwerking.

Iets anders is het als personen of afdelingen gebruik maken van ongeautoriseerde (zelfgebouwde) programma's, scripts of databases om bepaalde werkzaamheden te vergemakkelijken. Over het algemeen zullen dit soort programma's, scripts en databases niet groot genoeg zijn om te kwalificeren als grootschalige verwerking. Dat neemt niet weg dat het College als verwerkingsverantwoordelijke aanvullende regels kan stellen aan het gebruik van ongeautoriseerde programma's, scripts en databases aangezien dit de controle op rechtmatige gegevensverwerking bemoeilijkt.

Een belangrijke maatregel waarmee kan worden voorkomen dat de rechtmatigheid van bepaalde verwerkingen van persoonsgegevens (in digitale systemen) niet kan worden gewaarborgd, is het voorkomen dat persoonsgegevens onnodig worden gekopieerd. Het is algemeen bekend dat digitale gegevens zich eenvoudig laten vermenigvuldigen. Voor een goed beheer van gegevens is het noodzakelijk dat er een gezaghebbend document wordt aangewezen als origineel of bron. Dit origineel is doorslaggevend als er verschillende versies van dezelfde documenten in omloop zijn. Het is niet geheel duidelijk of de loggingsverplichting zich ook uitstrekt tot kopieën van de persoonsgegevens. In plaats van de loggingsverplichting uit te breiden naar alle programma's en plekken waarbij kopieën worden verwerkt, ligt het hoe dan ook meer in de rede de mogelijkheden te beperken om kopieën van gegevens te maken en deze buiten het bronsysteem om te raadplegen, te bewerken en te verstrekken. Als beleid wordt gemaakt en uitgevoerd om het overbodig kopiëren

van gegevens te voorkomen, is het niet nodig om in de systemen waarbij deze overbodige kopieën worden gebruikt een loggingsverplichting in te bouwen. Deze systemen behoren niet langer te worden gebruikt.

3.4 OM als verwerker

Alleen een verwerkingsverantwoordelijke kan opdracht geven aan de beheerders van systemen voor geautomatiseerde verwerking om logbestanden van verwerkingen te laten opstellen. Door het openbaar ministerie worden regelmatig strafrechtelijke persoonsgegevens verwerkt, terwijl het College niet de verwerkingsverantwoordelijke is (of lijkt te zijn). Het gaat dan om het raadplegen of zelfs wijzigen of toevoegen van persoonsgegevens in systemen van ketenpartners. Denk aan het raadplegen van de justitiële documentatie die wordt beheerd door Justid of het raadplegen van en toevoegen van informatie aan het politieregistratiesysteem BOSZ. Het is wenselijk dat door het openbaar ministerie met deze partners afspraken worden gemaakt over de logging van verwerkingen in deze systemen. Gesteld kan worden dat de uitvoering van deze afspraken primair de verantwoordelijkheid is van de verwerkingsverantwoordelijken van deze systemen. De verwerker kan er weliswaar aan bijdragen dat het onderwerp logging op de agenda komt te staan, maar is niet degene die de opdracht moet geven tot aanpassing van de systemen waarmee de gegevens worden verwerkt.

3.5 Conclusie

Het College van procureurs-generaal is als verwerkingsverantwoordelijke verantwoordelijk voor het voldoen aan de loggingsverplichting. Er moet voldaan zijn aan drie eisen: 1) het gaat om de verwerking van strafrechtelijke persoonsgegevens, 2) de verwerking moet plaatsvinden in systemen voor geautomatiseerde verwerking en 3) het College moet het gezag hebben over het beheer van deze systemen.

De belangrijkste afbakening van de loggingsverplichting is gekoppeld aan de tweede eis. De betekenis van het begrip geautomatiseerd systeem / systeem voor geautomatiseerde verwerking is onduidelijk. Het College heeft de vrijheid om dit begrip nader uit te leggen. Een redelijke uitleg is dat onder systemen voor geautomatiseerde verwerking wordt begrepen: programma's waarin grootschalig persoonsgegevens worden vastgelegd, gewijzigd en gecombineerd. Het gaat om programma's waarin op grootschalige wijze: zaaksgegevens worden verwerkt, persoonsdossiers van bij het strafrecht betrokken personen worden verwerkt of op andere wijze strafrechtelijke persoonsgegevens worden verwerkt.

Vanuit de doelen van de loggingsverplichting kan aan het bovenstaande nog worden toegevoegd dat logging primair van toegevoegde waarde is als de gebruikte persoonsgegevens rechtstreeks invloed kunnen hebben op de beslissingen die door de officier van justitie en/of de rechter worden genomen in een strafzaak. Ook kan worden gedacht aan verwerkingen die rechtstreeks gevolgen hebben voor de personen van wie de strafrechtelijke persoonsgegevens

worden verwerkt. Juist in deze gevallen kan logging een middel zijn om te voorkomen dat personen schade lijden als gevolg van het gebruik van onjuiste of onrechtmatig verwerkte persoonsgegevens.

4 Inhoud loggingsverplichting

4.1 Categorieën verwerkingen

De loggingsverplichting ziet volgens artikel 25 lid 1 Richtlijn en artikel 26e lid 1 Wjsg op het bijhouden/vastleggen van de volgende verwerkingen: het verzamelen, wijzigen, raadplegen, verstrekken onder meer in de vorm van doorgiften, combineren en vernietigen van persoonsgegeven. Het begrip verstrekking staat overigens niet in de Richtlijn, daarin wordt gesproken over bekendmaking – in het Engels *disclosure*. Met bekendmaking wordt in de Richtlijn bedoeld het doorgeven en ter beschikking stellen van strafrechtelijke persoonsgegevens aan personen of organisaties anders dan die van de verwerkingsverantwoordelijke. Deze definitie van verstrekken is voor de logging niet erg hanteerbaar. Een beter alternatief lijkt te zijn: **verstrekken is het uit het systeem halen (extraheren of kopiëren) van de persoonsgegevens**. In het onderstaande wordt uitsluitend het begrip verstrekken gebruikt om deze verwerking aan te duiden.

Zoals in het onderstaande nader wordt toegelicht, kunnen er twee categorieën verwerkingen worden onderscheiden. **Dit zijn categorie 1: de verwerkingen 'raadplegen' en 'verstrekken', en categorie 2: de verwerkingen 'verzamelen/vastleggen', 'wijzigen', 'combineren' en 'vernietigen'.** In het navolgende wordt hieraan ook gerefereerd als categorie 1-verwerkingen en categorie 2-verwerkingen. Deze twee categorieën verwerkingen vallen samen met een onderscheid dat bij de aanpassing van onder meer GPS is gemaakt tussen enerzijds 'logging' (categorie 1) en anders 'journalling' (categorie 2).

4.2 Soorten informatie in logbestand

<u>Categorie 1-verwerkingen</u>

Volgens artikel 25 lid 1 Richtlijn maken 'de logbestanden van raadpleging en bekendmaking (...) het mogelijk de redenen, de datum en het tijdstip van die handelingen te achterhalen en indien mogelijk de identiteit van de persoon die persoonsgegevens heeft geraadpleegd of bekendgemaakt, en de identiteit van de ontvangers van die persoonsgegevens.'[4] De Richtlijn geeft daarmee een indicatie welke informatie in het logbestand van categorie 1-verwerkingen moet staan. Er kan onderscheid worden gemaakt tussen de verschillende soorten informatie die uit de logbestanden van categorie 1-verwerkingen moet kunnen worden afgeleid: 1) de redenen van de handelingen, 2) de datum en het tijdstip van de

[4] Opvallend genoeg staat een vergelijkbare zinsnede niet in artikel 26e Wjsg, maar uitsluitend in de memorie van toelichting, *Kamerstukken II*, 34 889, nr 3 (MvT), p. 85.

handelingen, 3) de identiteit van de raadpleger en verstrekker en 4) de identiteit van de ontvanger. In het algemeen valt op dat in de Richtlijn deze vier soorten informatie alleen worden gekoppeld aan de logbestanden van de raadpleging en verstrekking. De logbestanden hoeven voor de overige verwerkingen dus niet per se deze informatie te bevatten. Nog een aanvullende opmerking over 1, 3 en 4.

1) Wat betreft de redenen staat in de preambule van de Richtlijn onder 57: "De identificatie van de persoon die persoonsgegevens heeft geraadpleegd of bekendgemaakt, dient te worden geregistreerd en op basis daarvan moeten de redenen voor de verwerkingsactiviteiten kunnen worden vastgesteld".[5] De redenen moeten dus worden afgeleid uit de persoon van de verwerker. Dit kan op twee manieren: als de raadpleging of verstrekking (en naar mag worden aangenomen ook de overige verwerkingen) onderdeel uitmaken van de reguliere werkzaamheden van de raadpleger of verstrekker, dan zijn deze reguliere werkzaamheden de reden van de verwerking. Als de raadpleging of verstrekking niet onderdeel uitmaken van de reguliere werkzaamheden, dan zal aan de betreffende persoon navraag moeten worden gedaan naar de reden voor de raadpleging of verstrekking. **Kortom: de reden zelf hoeft niet te worden gelogd, maar kan worden afgeleid uit de identiteit van de raadpleger of verstrekker – of tijdens een controle worden nagevraagd.**

> *In de Business Requirements (LOG.02) staat dat de gebruiker zelf de redenen voor de verwerking zou moeten invullen als dit niet automatisch kan worden afgeleid. Dit volgt niet uit de Richtlijn en kan worden gezien als een overbodige administratieve handeling.*

De Art. 29 Data Protection Working Party (WP29) kent een vergelijkbare insteek. WP29 overweegt dat "there has to be something in the logs explaining the reason why an individual accessed that log or record. In the view of the WP29, this obligation can best be fulfilled by ensuring that any automated processing systems and their respective logging elements are developed in accordance with the "data protection by design" requirements".[6] Als de toegang tot persoonsgegevens en de verwerking daarvan beperkt is tot bevoegde personen, hoeft degene die de verwerking uitvoert geen reden te geven. Die reden zit dan in beginsel al in de bevoegdheid. Een onbevoegd persoon die verwerkingen uitvoert, zal hier in de regel geen goede reden voor hebben. Welke reden deze persoon wel heeft, zal bij navraag moeten blijken.

3) Uit de Richtlijn volgt dat alleen de identiteit van de raadpleger en verstrekker van persoonsgegevens moet kunnen worden vastgesteld. Dat betekent dat het niet verplicht is om vast te leggen wie andere verwerkingshandelingen heeft verricht. De WP29 stelt dit ook vast, maar acht het niettemin wenselijk dat "the identification of the individual user should not be limited to the operations of

---

[5] Geciteerd in *Kamerstukken II*, 34 889, nr 3 (MvT), p. 85.

[6] Article 29 Data Protection Working Party, 'Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)', 29 november 2017, p. 27.

consultation and disclosure, but foreseen for all processing operations and include every person involved".[7] Hiermee wordt dus meer gevraagd dan wettelijk verplicht.

Het ontbreken van een wettelijke plicht biedt ruimte voor een genuanceerde en pragmatische benadering. In beginsel kan worden volstaan met alleen het loggen van degene die raadpleegt en verstrekt. Als vervolgens blijkt dat er andere verwerkingen onrechtmatig hebben plaatsgevonden, kunnen de loggegevens van degene die heeft geraadpleegd én kan bewerken wel worden gebruikt om te achterhalen welke persoon hoogstwaarschijnlijk de onrechtmatige verwerkingen heeft uitgevoerd. Om deze beoordeling te vergemakkelijken is het **wenselijk een onderscheid te maken tussen raadplegers die geen mogelijkheid hebben categorie 2-verwerkingen uit te voeren, en raadplegers die (een aantal van) deze bevoegdheden wel hebben.** Bij controle op onrechtmatige verwerkingen hoeven aan de 'alleen-raadplegers' geen vragen te worden gesteld over de mogelijk onrechtmatige andere verwerkingen.

4) Zolang de verstrekking van persoonsgegevens binnen de kaders van een systeem (d.w.z. met behulp van een programma) gebeurd, is het noodzakelijk dat zowel wordt vastgelegd wie de verstrekker is als wat de identiteit is van de ontvanger van de persoonsgegevens. Het is echter onmogelijk elke verstrekking te loggen. Zeker wanneer de persoonsgegevens buiten het systeem om op andere wijze worden vastgelegd – door het handmatig overschrijven van gegevens, door de gegevens te fotograferen of een screenshot te maken – kan noch de verstrekking noch de ontvanger worden gelogd. Het College kan als verwerkingsverantwoordelijke bepalen dat deze vormen van vermenigvuldigen van persoonsgegevens onwenselijk zijn, en dat deze daarom niet worden toegestaan.

<u>Categorie 2-verwerkingen</u>

Wat betreft categorie 2-verwerkingen is het wenselijk dat het volgende wordt gelogd: 1) de datum en het tijdstip van de verwerking, 2) de inhoud van de verwerking – wat is vastgelegd, gewijzigd, gecombineerd en/of vernietigd. Steeds zal het verschil duidelijk moeten zijn tussen de oude en de nieuwe situatie. Het is wenselijk dat categorie 2-verwerkingen kunnen worden gekoppeld aan een persoon. Dit hoeft echter niet uit het logbestand zelf te blijken. Wie hoogstwaarschijnlijk de bewerking heeft uitgevoerd, kan worden vastgesteld door de logbestanden over de categorie 2-verwerkingen te combineren met de logbestanden over de raadplegingen. Dat is geraadpleegd, impliceert de mogelijkheid van de andere verwerkingen.

> *In de Business Requirements (LOG.02) staat dat voor de verwerkingen verzameling/vastlegging, wijziging, combinatie en vernietiging zou moeten worden gelogd: de identiteit van de persoon die heeft verwerkt (inclusief*

[7] Article 29 Data Protection Working Party, 'Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)', 29 november 2017, p. 27.

functie en gebruikersrol) en de redenen voor de verwerking. Dit is niet niet correct, dit hoeft in beginsel niet te worden gelogd - zolang dit maar blijkt uit de logbestanden van categorie 1-verwerkingen.

4.3 Niveau registratie

Er moet ook worden bepaald op welk inhoudelijk niveau de registratie moet plaatsvinden. Gaat het om de verwerking van elk persoonsgegeven op zichzelf, of kan worden volstaan met het loggen van de verwerkingen van clusters aan persoonsgegevens? Het antwoord op deze vraag kan worden gezocht in het doel van de loggingsverplichting in combinatie met de categorieën verwerkingen. Het doel is - zoals gezegd - het mogelijk maken van interne controles op de juistheid en rechtmatigheid van de verwerkingen. Gezien dat doel is het wenselijk dat er onderscheid wordt gemaakt tussen de verschillende categorieën verwerkingen. Bij categorie 2-verwerkingen is het wenselijk om meer op detailniveau vast te leggen hoe de verwerking heeft plaatsgevonden. Bij categorie 1-verwerkingen is een algemener niveau net zo geschikt.

Categorie 1-verwerkingen

Voor de verwerkingen raadplegen en verstrekken kan worden volstaan met logging op hoofdlijnen. Het is voldoende dat op het niveau van zaak/dossier/registratienummer/scherm wordt gelogd - en dus niet op het niveau van documenten. Het is niet nodig dat de raadpleging of verstrekking van elk persoonsgegeven wordt bijgehouden. De toegevoegde waarde daarvan is zeer klein, omdat de verwerkingen op zaaksniveau vaak hetzelfde zijn - de hele zaak wordt geraadpleegd of verstrekt. Op het niveau van de zaak/dossier kan dus worden vastgelegd: i) wie heeft geraadpleegd of verstrekt, ii) op welke datum en tijdstip is geraadpleegd en verstrekt en iii) aan wie is verstrekt. Wat betreft i) kan het logbestand eventueel worden gecombineerd met een lijst van medewerkers waarin ook functietitels en bevoegdheden staan. Het is niet strikt noodzakelijk dat dit in het logbestand staat, zolang het daar maar uit kan worden afgeleid.

In de Business Requirements (LOG.02) staat dat gegevens moeten worden gelogd op basis waarvan de functie van de persoon die de verwerking uitvoert kan worden bepaald en de gebruikersrol. Dit moet zo worden uitgelegd dat dit moet kunnen worden achterhaald, niet dat deze informatie per se tot het logbestand zou moeten horen.

Categorie 2-verwerkingen

Voor de verwerkingen verzameling/vastlegging, wijziging, combinatie en vernietiging is het wel van belang dat op het niveau van de individuele persoonsgegevens wordt gelogd. Het is goed voorstelbaar dat deze verwerkingen kunnen verschillen voor de persoonsgegevens binnen een zaak/dossier, en zelfs binnen een document of registratieveld. Zo kan bijvoorbeeld wel het adres van een verdachte worden gewijzigd, maar zijn telefoonnummer niet.

Ten aanzien van het niveau van registratie kan verder nog worden opgemerkt dat de behoeften van degene die in de praktijk gebruik maken van de loggegevens van belang zijn. Indien blijkt dat er problemen ontstaan om te bewijzen dat bepaalde personen onrechtmatig gegevens hebben verwerkt doordat er te weinig is gelogd, kan dit een overweging zijn om bij categorie 1-verwerkingen wel op gegevensniveau te loggen of meer informatie in het logbestand op te nemen.

5 Bewaartermijnen

In artikel 25 Richtlijn staat niet hoe lang logbestanden moeten worden bewaard. Dit is evenmin opgenomen in artikel 26e Wjsg. In de memorie van toelichting bij de implementatie van de Richtlijn overweegt de wetgever: "De richtlijn gegevensbescherming opsporing en vervolging bevat geen bewaartermijn voor de logging, gelet op het doel van de gegevensverwerking is de verordening gegevensbescherming op die gegevens van toepassing. (...) De verwerkingsverantwoordelijke dient de bewaartermijn voor de gelogde gegevens vast te stellen in overeenstemming met de verordening gegevensbescherming. Het ligt in de rede de bewaartermijn te koppelen aan de periodieke privacy audits (art. 33 Wpg). Voor deze audits geldt een termijn van vier jaar (art. 6:5, eerste lid, Bpg)."[8]

De suggestie voor de bewaartermijn van de wetgever in de memorie van toelichting kan worden bekritiseerd. Waarom de Algemene verordening gegevensbescherming (AVG) van toepassing zou zijn op de loggingsgegevens wordt niet uitgelegd. De toepassing is niet zonder meer vanzelfsprekend. Aangezien de logging mede is bedoeld om de strafrechtelijke procedures te waarborgen, gaat het bij de logging uiteindelijk om verwerking 'met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten'. Immers, de rechtmatigheid van de verwerking van strafrechtelijke persoonsgegevens is een onderwerp dat zonder meer aan de orde kan komen tijdens de afdoening van een strafbaar feit. Zogezien zijn de loggegevens eerder strafrechtelijke persoonsgegevens waarop de Richtlijn van toepassing is. Dat geldt in ieder geval voor de logbestanden van categorie 2-verwerkingen. Zie hierover verder in paragraaf 5.

Het is zinvol naar andere aanknopingspunten voor de duur van de bewaartermijn te zoeken. In het commentaar WP29 op de Richtlijn wordt een andere richting gewezen voor wat betreft de lengte van de bewaartermijn:[9]

---

[8] *Kamerstukken II*, 34 889, nr 3 (MvT), p. 85.

[9] Article 29 Data Protection Working Party, 'Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)', 29 november 2017, p. 27-28.

> *"The Directive does not set any requirement on the storage period for logs. Therefore, in the view of the WP29, national legislators should provide for adequate storage periods by giving clear criteria or setting fixed periods.*
>
> *An adequate storage period for logs has to be derived from the purposes of logging as laid down in Article 25 (2) and should ensure that it is possible to achieve those purposes. This goes especially for the verification of the lawfulness of the processing, which lies within the tasks of the DPAs. Therefore, the storage period for logs should give DPAs enough time to retrace and review the data processing.*
>
> *In the view of the WP29, the monitoring of access to data i.e. consultation and disclosure should be done on a regular basis and within a shorter period of time. In general, it is not necessary to keep the logs on access as long as the underlying data are stored.*
>
> *As for the logs on the history of data i.e. collection, alteration, combination and deletion, a different approach may be adequate depending on the database in question.*
>
> *Deciding on appropriate storage periods, it should be taken into account that on the one hand, a long storage period for logs will help to keep trace of the history of the processing (with a benefit for the data subject, the quality of data and the security measures). In criminal procedures or for preventive purposes the underlying data are usually stored over a long period and often the data subject only gains knowledge of the processing at a later stage. At this point it should be possible to retrace the data processing by means of the logs. On the other hand, keeping the logs after deletion of the underlying data implies that part of the information is also retained for longer than the storage period foreseen. This would call for a shorter storage period of logs. In conclusion, the right balance should be found on a case-by-case basis."*

De WP29 maakt eenzelfde onderscheid tussen categorie 1-verwerkingen: raadplegen en verstrekken en categorie 2-verwerkingen: verzameling/vastleggen, wijziging, combinatie en vernietiging. De logbestanden van de verwerkingen uit categorie 1 hoeven niet zo lang te worden bewaard als de logbestanden van verwerkingen uit categorie 2.

Over categorie 1-verwerkingen zegt de WP29 dat de rechtmatigheid van de verwerkingen regelmatig moet worden gecheckt, en dat de logbestanden daarom niet zolang hoeven te worden bewaard als de onderliggende bestanden. **Voor de logbestanden over categorie 1-verwerkingen kan een bewaartermijn van vier jaren worden aangehouden.**

Over categorie 2-verwerkingen zegt de WP29 dat het wenselijk kan zijn de logbestanden veel langer te bewaren. Om te controleren welke verwerkingen er plaats hebben gevonden in een zaak/dossier is het wenselijk dat op een later moment kan worden teruggezocht welke gegevens bijvoorbeeld zijn gewijzigd of

vernietigd. Tegelijkertijd wijst de WP29 erop dat hiermee vernietigde gegevens ook langer bewaard blijven, omdat ze onderdeel uit blijven maken van de logbestanden. De WP29 komt uiteindelijk niet verder dan dat per individuele zaak de bewaartermijn zou moeten worden bepaald. Dit is echter geen werkbare oplossing.

Het is in ieder geval wenselijk de logbestanden voor categorie 2-verwerkingen te bewaren tot het strafbare feit definitief is afgedaan, door een onherroepelijke rechterlijke uitspraak of sepotbeslissing. Indien er geen afdoeningsbeslissing is genomen, moeten de logbestanden in ieder geval bij de verjaringstermijn van het feit worden vernietigd. Voor zover strafrechtelijke persoonsgegevens ook in de executiefase nodig is, kan worden nagedacht over het bewaren van de logbestanden voor de periode van executie. De logbestanden voor categorie 2-verwerkingen worden mede bewaard om de strafrechtelijke procedures te waarborgen. Zolang de strafrechtelijke procedure niet is afgelopen, kan het dus nodig zijn de categorie 2-verwerkingen terug te zoeken om na te gaan wat er in de zaak is gebeurd. Overigens is het mogelijk dat na verloop van tijd het niet meer mogelijk is te achterhalen wie verantwoordelijk is voor bepaalde verwerkingen, omdat de logbestanden van categorie 1-verwerkingen eerder zijn vernietigd. Dit is aanvaardbaar. Het doel van het bewaren van de logbestanden van categorie 2-verwerkingen is na verloop van tijd niet meer zozeer het achterhalen van misbruik, maar eerder het garanderen van de juistheid van de opgeslagen persoonsgegevens. In overleg zal moeten worden bepaald hoe deze bewaartermijn kan worden geoperationaliseerd.

6 Inzage betrokkene in logbestanden

Het maken van een logbestand kan op zichzelf ook een verwerking van persoonsgegevens zijn. Dit roept een aantal vragen op: Welke persoonsgegevens worden in de logbestanden verwerkt? Vallen deze logbestanden onder de AVG of Richtlijn? Heeft de betrokkene wiens persoonsgegevens worden verwerkt recht op inzage van de logbestanden?

1) Welke persoonsgegevens worden in de logbestanden verwerkt?
Er kunnen twee soorten persoonsgegevens in de logbestanden worden verwerkt. In de eerste plaats de persoonsgegevens van de raadpleger of verstrekker. Dit is in de regel een OM-medewerker, maar kan ook een extern persoon zijn die toestemming heeft gekregen om persoonsgegevens in OM-systemen te raadplegen. Als – zoals hierboven is gesteld – voor categorie 2-verwerkingen niet apart wordt bijgehouden wie de verwerking heeft verricht, bevatten de logbestanden van deze verwerkingen in beginsel niet de persoonsgegevens van de persoon die de verwerking uitvoert. In de tweede plaats kunnen de logbestanden de persoonsgegevens bevatten van de persoon van wie de gegevens worden verwerkt. Door het verschil tussen de oude en de nieuwe situatie te loggen, kunnen persoonsgegevens van de verdachte, getuigen of andere betrokkenen worden gelogd. Denk aan het verschil tussen het oude en het nieuwe adres van

de verdachte.

2) Vallen de logbestanden onder de AVG of Richtlijn?

Onder welk regime de verwerking van persoonsgegevens valt, hangt in de eerste plaats af van het doel van de verwerking. Bij de afweging moet ook het karakter van de verwerkte persoonsgegevens worden meegewogen en de persoon op wie de gegevens betrekking hebben worden meegenomen. Het rechtstreekse doel van de verwerking is het mogelijk maken van de controle op de rechtmatigheid van de verwerkingen. Dit is op zichzelf geen strafrechtelijk doel. Het achterliggende doel van een rechtmatige verwerking is echter wel geheel strafrechtelijk, te weten het nemen van juiste en rechtmatige beslissingen bij de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten.

Wordt gekeken naar het karakter van de verwerkte persoonsgegevens en de persoon op wie die gegevens betrekking hebben, dan is duidelijk dat categorie 2-verwerkingen onder de Richtlijn vallen. Als persoonsgegevens worden verwerkt met het oog op de opsporing en vervolging van strafbare feiten, dan moet het logbestand waar deze zelfde gegevens instaan ook onder de Richtlijn vallen. Anders zouden op precies dezelfde gegevens twee regimes van toepassing zijn. Als bijvoorbeeld het adres van de verdachte wordt gewijzigd – en in het logbestand het oude adres nog is te vinden – is het evident dat al deze gegevens zijn verzameld en verwerkt in het kader van de opsporing en vervolging van strafbare feiten.

Wat betreft de categorie 1-verwerkingen is een ander standpunt mogelijk. Bij deze verwerkingen gaat het om de persoonsgegevens van OM-medewerkers en andere personen met toegang tot OM-systemen. De verwerking van deze persoonsgegevens raakt in principe niet aan de opsporing en vervolging van strafbare feiten. Dat wordt pas anders als de betrokken persoon strafrechtelijk wordt aangesproken op een onrechtmatige verwerking. Daarom kan worden gesteld dat de persoonsgegeven in logbestanden van categorie 1-verwerkingen in beginsel onder de AVG vallen.

3) Heeft de betrokkene wiens persoonsgegevens worden verwerkt recht op inzage van de logbestanden?

Omdat onderscheid is gemaakt tussen het toepasselijke regime voor de logbestanden van categorie 1-verwerkingen en categorie 2-verwerkingen, moet voor dit antwoord onderscheid worden gemaakt tussen beide verwerkingen.

Voor categorie 1-verwerkingen is het denkbaar dat OM-medewerkers en andere personen met toegang tot OM-systemen willen weten welke gegevens het OM over hun verwerkt. In dat geval kan de betrokken persoon op grond van de AVG vragen welke gegevens het OM over hem of haar heeft verwerkt. Deze gegevens kunnen alleen worden opgevraagd door de OM-medewerker, niet door de persoon van wie de persoonsgegevens zijn geraadpleegd of verstrekt.

Voor categorie 2-verwerkingen is het mogelijk dat een verdachte wil weten of de verwerkingen rechtmatig zijn gebeurd. In dat geval zijn de regels over de verstrekking van processtukken (die volledig samenvallen met de regels

voor inzage in de Wjsg) van toepassing. Het is denkbaar dat de verdediging op grond van artikel 34 Sv verzoekt om inzage in de logbestanden om te onderzoeken of er onterechte wijzigingen hebben plaatsgevonden van de geregistreerde gegevens. Dit verzoek hoeft alleen te worden ingewilligd als er aanwijzingen zijn dat er onrechtmatige handelingen hebben plaatsgevonden of onjuiste gegevens zijn vastgelegd. Bij inzage hoeft de naam van de raadpleger of verwerker in beginsel niet te worden verstrekt.

7 Gebruik logbestanden

In paragraaf 2 is al benoemd dat de logging van verwerkingen van strafrechtelijke persoonsgegevens geen doel op zichzelf is, maar een middel om te controleren of het openbaar ministerie strafrechtelijke persoonsgegevens op behoorlijke, rechtmatige, doelgebonden, proportionele en subsidiaire wijze verwerkt. De logbestanden kunnen worden gebruikt om misbruik op te sporen. Het is noodzakelijk dat dit ook wordt gedaan. Als logbestanden niet worden gebruikt – om misbruik op te sporen (categorie 1-verwerkingen) of om de juistheid en integriteit van gegevens te controleren (categorie 2-verwerkingen) – heeft logging geen zin.

De logging is primair bedoeld voor interne controles binnen het openbaar ministerie. Onder meer de functionaris gegevensbescherming (FG) heeft als taak om toezicht te houden op de naleving van de gegevensbeschermingsregels (artikel 25f i.c.m. 39r Wjsg en artikel 34 Richtlijn). De logbestanden kunnen worden gebruikt om te controleren of onbevoegde personen verwerkingen hebben verricht. Als dit het geval is, kunnen daar consequenties aan worden verbonden. Het is wenselijk dat verder wordt uitgewerkt op welke wijze de controles op de rechtmatigheid van de verwerkingen vorm gaan krijgen door de FG en andere interne controleurs en welke consequenties zullen worden verbonden aan de vaststelling van onrechtmatige verwerkingen.

Openbaar Ministerie

Informatiebeveiligingsbeleid 2023

Vaststelling

Versie	1.0		
Datum vaststelling		Vervaldatum	

Paraaf

Mr. F.M. Damme

Procureur-generaal tevens CIO Openbaar Ministerie

Documenthistorie

BR

Inhoud

DEEL I – Informatiebeveiligingsbeleid Openbaar Ministerie 7

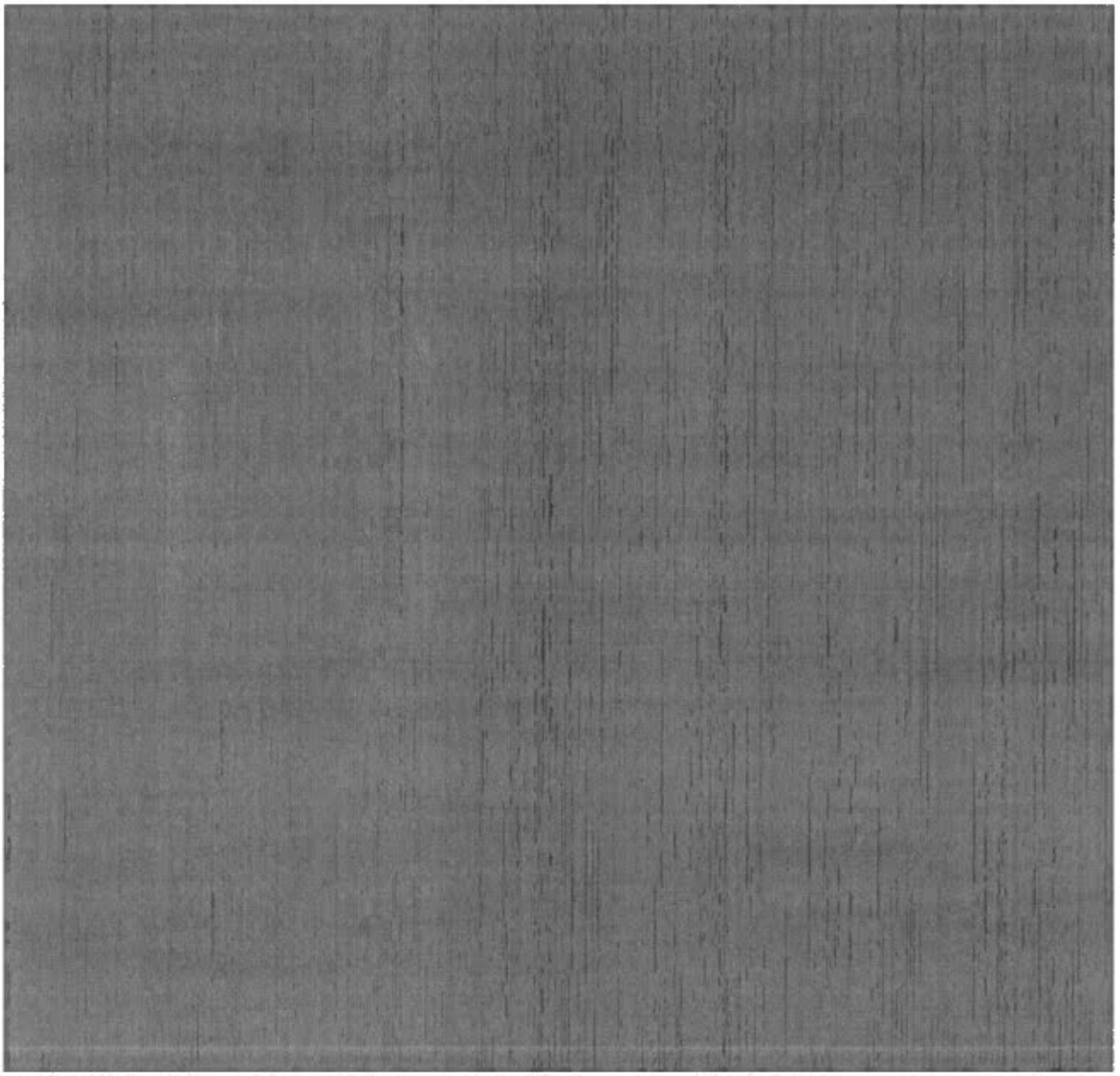
1. Inleiding 7

1.1. Doel 8

1.2. Doelgroep 9

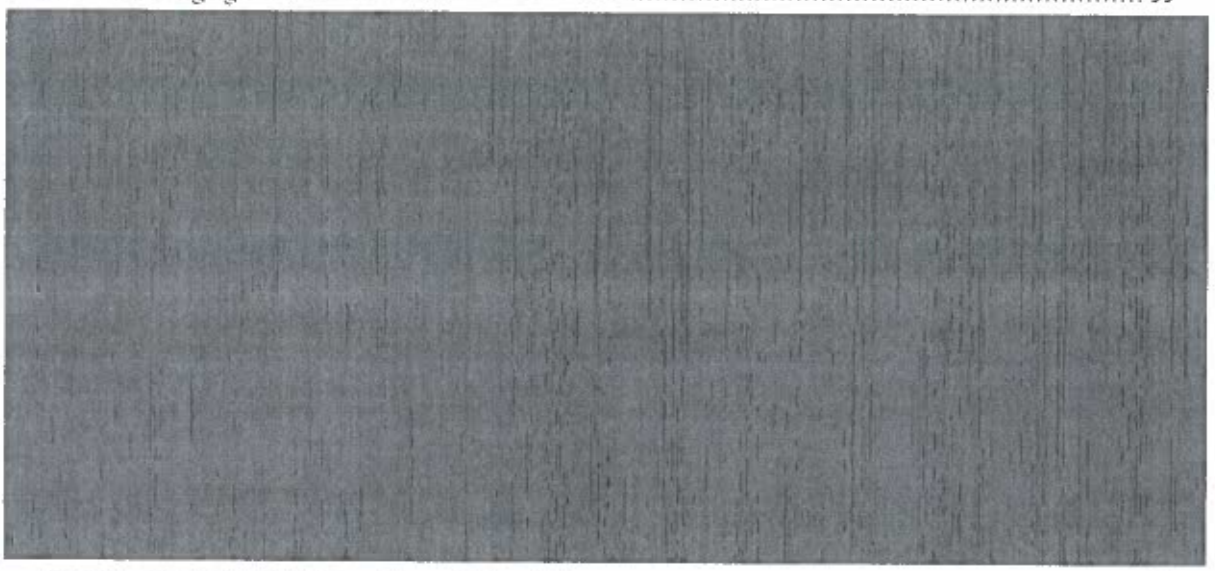
1.3. Scope 9

BR



BR

5.3. Beveiliging en Personeel 35



BR

DEEL IV – Tactische Richtlijnen Informatiebeveiliging 63

6. Informatiebeveiligingsbeleid – Tactische richtlijnen 63

6.1. Toegangsbeveiliging – IBB-TR05 64

6.1.1. Uitgangspunten 64

6.1.2. Randvoorwaarden 64

6.1.3. Standaarden en regels voor logische toegangsbeveiliging 65

BR

DEEL I

Informatiebeveiligingsbeleid van het Openbaar Ministerie

DEEL I – Informatiebeveiligingsbeleid Openbaar Ministerie

1. Inleiding

Het OM is verantwoordelijk voor het opsporen en vervolgen van strafbare feiten. Het werk van het OM is erop gericht dat daders een passende straf krijgen, dat slachtoffers en nabestaanden het gevoel hebben dat er iemand naast hen staat, en dat de samenleving voelt dat het recht bij het OM in goede handen is. De hoofdtaken van het OM zijn: het leiding geven aan de politie bij het opsporen van strafbare feiten, strafbare feiten vervolgen en verdachten voor de rechter brengen en het afdoen van strafbare feiten zonder tussenkomst van een rechter. Het Openbaar Ministerie (OM) is als onderdeel van het ministerie van Justitie en Veiligheid een belangrijke partner in de strafrechtketen en wordt door de maatschappij gezien als een betrouwbare en integere organisatie, die informatie over burgers en bedrijven op integere wijze verwerkt in overeenstemming met geldende wet- en regelgeving. Informatie kent binnen de strafrechtketen vele verschijningsvormen, van gesproken woord en papieren dossier tot vergaande digitale verwerking van gegevens. De betrouwbaarheid van de OM-informatiesystemen en OM-gegevens dient in overeenstemming te zijn met het beeld dat de maatschappij van het Openbaar Ministerie heeft. Informatiebeveiliging is daarmee een onmisbaar middel.

Informatiebeveiliging is in dit document gedefinieerd als het stelsel van maatregelen dat de organisatie treft om de beschikbaarheid, integriteit en vertrouwelijkheid van de OM-gegevens en de OM-informatiesystemen te waarborgen. De OM-informatiesystemen en de OM-gegevens, die daarmee/daarin worden verwerkt, zijn voor het Openbaar Ministerie essentiële productiemiddelen om haar doelstelling te bereiken. Namelijk dat handhaving van ons strafrecht essentieel is om te kunnen leven in een veilige en rechtvaardige maatschappij.

Dit document beschrijft het informatiebeveiligingsbeleid van het Openbaar Ministerie dat in afstemming met het MT IVOM door het College van procureurs-generaal is vastgesteld op [datum vaststelling invullen].

De toenemende digitalisering in de maatschappij maar ook in de strafrechtketen heeft consequenties voor informatiebeveiliging waarbij de aandacht voor de in te zetten of ingezette informatietechnologie meer aandacht vraagt, zonder de aandacht voor andere meer traditionele verwerkingen te verminderen. De continue ontwikkelingen binnen samenwerkingsverbanden in de strafrechtketen en toenemende inzet van nieuwe technologie o.a. als gevolg van de pandemie leiden ertoe dat dat informatiebeveiliging een steeds grotere uitdaging wordt. Een uitdaging die alleen kan worden aangepakt door voortdurend bij te blijven en te anticiperen op nieuwe (technologische, juridische en maatschappelijke) ontwikkelingen, waarbij in multidisciplinaire teams wordt samengewerkt om alle aspecten te belichten. Tot de multidisciplinaire teams worden naast materiedeskundigen ook privacy, security en bedrijfsvoering specialisten (bijvoorbeeld inkoopjuristen) gerekend.

Het voorliggend informatiebeveiligingsbeleid is onder andere gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO) en het Normenkader Beveiliging Rijkskantoren. De Baseline Informatiebeveiliging is de standaard voor Rijk, provincies, gemeenten en waterschappen. Het informatiebeveiligingsbeleid bestaat uit de volgende onderwerpen:

1. Beveiligingsbeleid

2. Beveiliging en Organisatie
3. Beveiliging en Personeel
4. Beveiliging en bedrijfsmiddelen
5. Toegangsbeveiliging
6. Cryptografie
7. Fysieke beveiliging en beveiliging omgeving
8. Beveiliging en Bedrijfsvoering
9. Communicatiebeveiliging
10. Acquisitie, ontwikkeling en onderhoud van informatiesystemen
11. Beveiliging en Leveranciers
12. Informatiebeveiligingsincidenten
13. Beveiliging en Bedrijfscontinuïteit
14. Naleving

In het informatiebeveiligingsbeleid OM worden globale richtlijnen gegeven, die zijn gebaseerd op "good practice". Hoofdstuk 2 "Informatiebeveiligingsbeleid Openbaar Ministerie" bevat het informatiebeveiligingsbeleid dat door het College van procureurs-generaal is vastgesteld. In de daarop volgende hoofdstukken worden vervolgens richtlijnen gegeven voor de verschillende (informatiebeveiligings-) onderwerpen.

Het Informatiebeveiligingsbeleid wordt periodiek (in principe elk jaar) geëvalueerd en waar nodig bijgesteld. In de evaluatie worden relevante wijzigingen in de omgeving van het OM beoordeeld en worden noodzakelijke aanpassingen in het informatiebeveiligingsbeleid doorgevoerd. De wijzigingen kunnen bestaan uit een veranderend dreigingsprofiel en nieuwe technologische, juridische en maatschappelijke ontwikkelingen.

Het Openbaar Ministerie bestaat uit onderling verschillende organisatieonderdelen (hierna parketten genoemd), waardoor de implementaties van de beveiligingsmaatregelen van elkaar kunnen verschillen. Het informatiebeveiligingsbeleid biedt echter een gemeenschappelijk kader voor alle parketten. De parketten zijn verantwoordelijk voor de invoering van het informatiebeveiligingsbeleid en kunnen indien zij dit nodig achten op basis van een risicoschatting besluiten om aanvullende beveiligingsmaatregelen te treffen.

1.1. Doel

Voorliggend informatiebeveiligingsbeleid is het kader voor passende fysieke, technische/logische en organisatorische/procesmatige maatregelen om OM-informatie en -informatiesystemen te beschermen en te waarborgen, zodanig dat risico's toereikend worden beheerst en dat het Openbaar Ministerie voldoet aan relevante wet- en regelgeving gerelateerd aan informatiebeveiliging.

Het Openbaar Ministerie streeft er naar om 'in control' te zijn en daarover op professionele wijze verantwoording af te (kunnen) leggen. In control zijn betekent in dit verband dat het Openbaar Ministerie weet welke maatregelen genomen zijn, dat er een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in de managementcyclus bestaande uit een Information Security Management System (ISMS) en Plan-Do-Check-Act-cyclus (PDCA-cyclus). Het Openbaar Ministerie accepteert de risico's voor die maatregelen die nog niet getroffen zijn.

1.2. Doelgroep

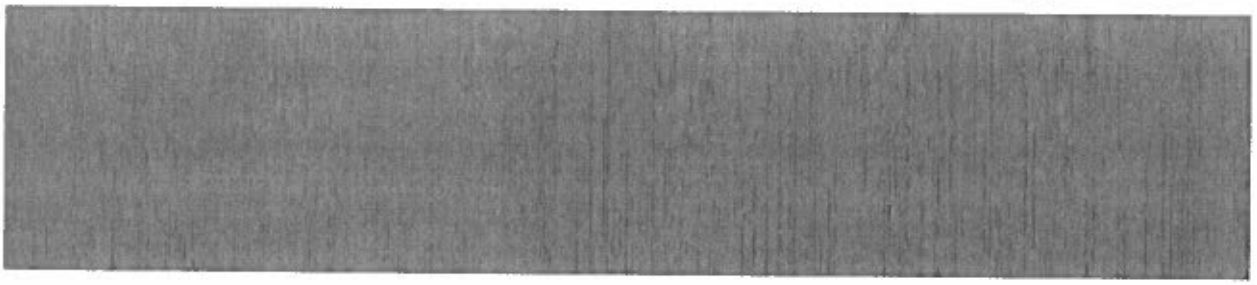
Dit document is van belang voor het management van het Openbaar Ministerie, het lijnmanagement van haar onderdelen, de gebruikers, de systeemeigenaren, applicatiebeheerders en de dienstverlenende ICT-uitvoeringsorganisatie.

1.3. Scope

Dit beleid is van toepassing op alle informatie verwerkende systemen en -processen binnen het Openbaar Ministerie waarmee gegevens, die onder de verantwoordelijkheid van het College van procureurs-generaal vallen, worden verwerkt. Het gaat hierbij om de reguliere productie-omgeving (waarin gegevens van het niveau departementaal vertrouwelijk kunnen worden verwerkt) en de hoger beveiligde omgeving (waarin gegevens die hoger gerubriceerd zijn dan departementaal vertrouwelijk of die aanvullende beschermingsmaatregelen behoeven kunnen worden verwerkt).

Dit beleid is ook van toepassing op de informatieverwerking, die door het Openbaar Ministerie is uitbesteed aan derden (bijvoorbeeld ICT-dienstenleveranciers). Dit beleid is niet van toepassing op de informatieverwerking vallend onder een samenwerkingsovereenkomst, waarbij een andere partij de verwerkingsverantwoordelijke is. Hierover dienen separaat afspraken te worden gemaakt die in een (samenwerkings-) convenant worden of zijn vastgelegd.

BR



Bladzijde 11 t/m 34 - BR

5.3. Beveiliging en Personeel

Het Openbaar Ministerie stelt eisen aan het uitoefenen van functies om de betrouwbaarheid en continuïteit van informatie en informatiesystemen te borgen. Hiertoe wordt in functieomschrijvingen rekening gehouden met de eventuele risico's die de uitvoering van de functie met zich meebrengt. Bij het OM zijn functies verdeeld in 'Standaardfuncties' en 'Vertrouwensfuncties' (in niveaus a, b of c). Afhankelijk van de te vervullen functie overlegt de medewerker een Verklaring omtrent Gedrag of Verklaring van geen Bezwaar.

IDnr	IBB-SR03
BIR / NkBR verwijzing	BIO 7
Titel	Personeel en informatieveiligheid
Omschrijving	
IBB-SR03.01	**Algemeen** Het College van Procureurs-Generaal heeft een lijst van vertrouwensfuncties voor het OM vastgesteld. De Minister van Binnenlandse Zaken heeft het aanwijzingsbesluit vertrouwensfuncties voor het Ministerie van Veiligheid en Justitie, betreffende het Openbaar Ministerie vastgesteld.
IBB-SR03.02	**Voorafgaand aan een dienstverband** Het Openbaar Ministerie draagt zorg dat medewerkers hun verantwoordelijkheden op het gebied van informatiebeveiliging begrijpen. Nieuwe medewerkers die een standaardfunctie gaan uitoefenen, overleggen vóór indiensttreding een Verklaring omtrent het gedrag (VOG), afgegeven door het Centraal orgaan Verklaring omtrent Gedrag (COVOG). Art. 3 lid 1 van de Wet op de veiligheidsonderzoeken (WVO) bepaalt dat personen die op een vertrouwensfunctie aangesteld gaan worden, een veiligheidsonderzoek moeten ondergaan voordat invulling aan de vertrouwensfunctie kan worden gegeven. Art. 5 lid 1 van de WVO bepaalt dat personen die een functie vervullen die nadien als een vertrouwensfunctie is aangewezen, alsnog een veiligheidsonderzoek moeten ondergaan. Het veiligheidsonderzoek gebeurt door de Algemene Inlichtingen en Veiligheidsdienst (AIVD) die bij positief resultaat een Verklaring van geen Bezwaar (VGB) afgeven. Het OM eist van medewerkers op vertrouwensfuncties een VGB vóórdat zij met hun werk beginnen. Bij de inhuur van medewerkers gelden de ARVODI. Elke ambtenaar in welke rechtsverhouding dan ook, heeft een geheimhoudingsplicht volgens artikel 2, lid 5 van de Algemene Wet

	Bestuursrecht (Geheimhoudingsverplichting). Elke ambtenaar gedraagt zich zoals een goed ambtenaar betaamt (art 50 ARAR) en is verplicht een eed of belofte af te leggen (art 51 ARAR). Voor externe medewerkers wordt een geheimhoudingsverklaring geëist, wanneer zij met vertrouwelijke informatie in aanraking kunnen komen. In de geheimhoudingsverklaring is de bepaling opgenomen dat de plicht tot geheimhouding van informatie doorloopt na afloop van de werkzaamheden.
IBB-SR03.03	**Gedurende het dienstverband** Het MT vereist van medewerkers dat zij beveiliging toepassen overeenkomstig vastgesteld beleid en vastgestelde procedures. Alle medewerkers van Openbaar Ministerie worden daarom met regelmaat geïnformeerd over ontwikkelingen op het gebied van informatiebeveiliging. Indien nodig worden trainingen of bijscholingen verzorgd. Voor zover relevant worden hierover afspraken vastgelegd in planningsgesprekken. Specifiek voor applicatieontwikkelaars zorgt Openbaar Ministerie voor een training in het ontwikkelen van veilige applicaties. De Rijksoverheid heeft een interne klokkenluidersregeling voor het melden van misstanden. Het Ministerie van VWS heeft een Meldprocedure integriteitsschendingen en misstanden ingericht. Openbaar Ministerie heeft vertrouwenspersonen aangewezen. Wanneer medewerkers inbreuk plegen op de beveiliging worden mogelijk formele disciplinaire maatregelen genomen, conform het Algemeen Rijksambtenarenreglement.
IBB-SR03.04	**Beëindiging van het dienstverband** De toegangsrechten van alle medewerkers tot informatie en IT middelen worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst, dan wel worden na wijziging van het dienstverband of de functie aangepast.
Gerelateerde documenten	• ARVODI • ARAR, Ambtenarenwet • Meldprocedure integriteitsschendingen • Model Integriteitsverklaring Rijk voor externen • Gedragsregeling voor de digitale werkomgeving
Motivering	Het voorkomen van menselijk falen en bedreigingen van menselijke aard significante invloed kunnen hebben op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie.
Voorbeeld	Tijdens de introductiedagen 'Welkom bij Openbaar Ministerie' wijst de CISO nieuwe medewerkers op hun verantwoordelijkheden
Mogelijke uitzondering	Bij externe inhuur van uitzendkrachten wordt de werkgever geacht een VOG in bezit te hebben.

Aanvullende beleidsregel(s) HBO	De functies van Security Officer en CISO zijn aangemerkt als vertrouwensfunctie, waarbij een minimale B-screening vereist is. De Security Officers moeten een VGB-screening hebben op hetzelfde niveau van de data, die wordt gebruikt in het uitvoeren van de werkzaamheden behorende bij deze functie.

Bladzijde 38 t/m 63 - BR

6.1. Toegangsbeveiliging – IBB-TR05

6.1.1. Uitgangspunten

Bij het ontwerpen, implementeren en gebruiken van logische toegangsbeveiliging dienen de volgende uitgangspunten gehanteerd te worden:

- Voor elk primair of ondersteunend proces, informatiesysteem en gegevensverzameling is een verantwoordelijke lijnmanager benoemd;
- De eigenaar van de gegevens is bevoegd toegang te verlenen;
- Er worden in de regel gepersonaliseerde[1] identiteiten gebruikt. Voor herleidbaarheid en transparantie is het namelijk nodig om te weten wie een bepaalde actie heeft uitgevoerd[2];
- Gegevens worden afgeschermd waar het kan en geautoriseerd waar het moet. Het houdt in dat alle data is afgeschermd en toegang wordt geboden door middel van autorisaties op basis van "need-to-know".
- Voor alle gebruikers vindt een logische toegangscontrole plaats voordat toegang wordt verleend tot informatiesystemen of gegevens die verwerkt worden met die informatiesystemen.

6.1.2. Randvoorwaarden

Onderstaande randvoorwaarden dienen ingevuld te worden met betrekking tot de logische toegangsbeveiliging.

- Het proces voor de uitgifte van de authenticatiemiddelen aan gebruikers is ingericht.
- Er is een overzicht van informatiesystemen beschikbaar en voor ieder informatiesysteem wordt aangegeven wie de systeemeigenaar is.
- Ten behoeve van de aanvraag, goedkeuring en vastlegging van autorisatieverzoeken voor medewerkers zijn overzichten beschikbaar, waarin wordt vastgelegd welke medewerkers autorisatieverzoeken mogen goedkeuren en welke medewerkers autorisatieverzoeken mogen verwerken in informatiesystemen. In het kader van functiescheiding mag de goedkeurende taak en de verwerkende taak niet door dezelfde medewerker worden uitgevoerd. De medewerkers die mogen goedkeuren worden vastgelegd in een mandaatregister, de medewerkers die de verwerkende taak uitvoeren worden vastgelegd in de autorisatiebeheerderslijst. Dit overzicht wordt opgesteld en actueel gehouden door de systeemeigenaar, eventueel in overleg met de gegevens- en/of proceseigenaar.
- Er is een overzicht van wel en niet toegestane combinaties van taken beschikbaar. Deze matrix bevat een overzicht van wel en niet toegestane combinaties van autorisaties binnen een informatiesysteem, die aan één medewerker mogen worden toegekend. In deze lijst dienen de rollen voor te komen die uit het oogpunt van functiescheiding belangrijk zijn. Dit overzicht wordt opgesteld en actueel gehouden door de systeemeigenaar, eventueel in overleg met de gegevens- en/of proceseigenaar. De systeemeigenaar dient bij het opstellen van een autorisatieprocedure rekening te houden met mogelijk van toepassing zijnde wet- en regelgeving.

[1] Onder gepersonaliseerde identiteiten wordt in het kader van dit beleid verstaan: identiteiten die herleidbaar zijn tot een natuurlijke persoon.
[2] Verplichting komt voort uit de privacywetgeving.

- Er is een overzicht, met daarin welke rollen en functies worden uitgevoerd door welke medewerker(s), beschikbaar. Deze autorisatiematrix bevat een overzicht van welke autorisaties aan één medewerker zijn toegekend. Dit dient per informatiesysteem of bedrijfsproces te worden geadministreerd. Dit overzicht wordt opgesteld en actueel gehouden door de systeem-, proceseigenaar of afdelingsmanager.

6.1.3. Standaarden en regels voor logische toegangsbeveiliging

In de volgende tabellen staan de te hanteren standaarden en regels ten aanzien van het het verlenen van toegang tot de gegevens, applicaties en ICT-infrastructuur van het Openbaar Ministerie.

IDnr	**IBB-TR05-LTB-R01**
BIO / NkBR verwijzing	BIO 12.4.1.1
Titel	Registratie van de digitale identiteit
Omschrijving	Zowel de persoonlijke[3] als de digitale identiteit van interne medewerkers moet worden geregistreerd in de systemen van toepassing. Voor externe medewerkers en medewerkers van ketenpartners dient enkel de digitale identiteit geregistreerd te zijn terwijl de persoonlijke identiteit geregistreerd is door de externe partij of ketenpartner.
Gerelateerde documenten	n.v.t.
Motivering	Identiteiten moeten geregistreerd staan om handelingen aan de verantwoordelijke personen te kunnen koppelen.
Voorbeeld	Jan Jansen werkt bij het Openbaar Ministerie. De digitale identiteit is de gebruikersnaam van Jan waarmee hij zich kenbaar maakt op het OM netwerk. Voorbeelden van fictieve gebruikersnamen zijn: NL123465 of JansJ01.
Mogelijke uitzondering	Voor bepaalde ketenpartners, bijvoorbeeld politie en Rechtspraak, heeft het OM andere afspraken gemaakt. Het OM registreert niet de persoonlijke identiteit van deze medewerkers en geeft hen op basis van de registratie bij Rechtspraak of politie een digitaal account bij het OM. De registratie van de persoonlijke identiteit gebeurt dan bij deze ketenpartners.

[3] Onder persoonlijke identiteit wordt in dit document verstaan; wettelijk identificatiedocument van de medewerker of gelijkwaardig document indien het over een buitenlands ingezetene gaat. Hierbij kan gebruik worden gemaakt van het RIN dat aan een persoon wordt gekoppeld.

IDnr	IBB-TR05-LTB-R02
BIO / NkBR verwijzing	BIO 12.4.1.1
Titel	Digitale identiteiten zijn herleidbaar tot natuurlijke personen
Omschrijving	De persoonlijke identiteit van interne medewerkers moet gekoppeld zijn aan de digitale identiteit in de systemen van toepassing. In het geval van externe accounts moet de ketenpartner de persoonlijke identiteit van de betrokken gebruiker vastgesteld hebben, zodat een koppeling gelegd kan worden tussen de persoonlijke en digitale identiteit.
Gerelateerde documenten	Nog op te stellen procedure voor aanvragen van groepsaccounts
Motivering	Iedere handeling door een digitale identiteit moet teruggekoppeld kunnen worden tot een natuurlijk persoon. Dit is niet alleen voor verantwoording, maar ook om mogelijke identiteitsdiefstal tegen te gaan.
Voorbeeld	Logregel laat de naar een natuurlijke persoon herleidbare gebruikersnaam zien die verzocht een handeling uit te voeren.
Mogelijke uitzondering	Wanneer een groepsaccount nodig is, dient de motivatie hiervoor vastgelegd en goedgekeurd worden. De genomen maatregelen worden gedocumenteerd om traceerbaarheid tot een natuurlijke persoon mogelijk te maken.

IDnr	IBB-TR05-LTB-R03
BIO / NkBR verwijzing	BIO 9.2.1.2
Titel	Functionele accounts
Omschrijving	De toegang tot informatie, informatiesystemen of de ICT-infrastructuur kan niet altijd één op één worden gekoppeld aan een natuurlijke persoon. Verschillende componenten binnen de informatievoorziening maken zelf gebruik van accounts om bij elkaar diensten af te nemen. Voorbeelden zijn: applicatie accounts, system accounts en service accounts. Daarnaast zijn er situaties waarin natuurlijke personen gebruik maken van een gedeeld account: cursus- en opleidingsaccounts in een lesomgeving. Voor de technische functionele accounts, zoals applicatie accounts, system accounts en service accounts, is de ICT-uitvoeringsorganisatie verantwoordelijk.

	Voor de overige niet-technische functionele accounts moet een natuurlijk persoon benoemd worden, die verantwoordelijk is voor het gebruik van het account. Deze persoon voert autorisatie-aanvragen uit en dient op de hoogte te zijn van de toekenning met bijbehorende verantwoordelijkheden en consequenties.
Gerelateerde documenten	
Motivatie	Iedere handeling door een digitale identiteit moet teruggekoppeld kunnen worden tot een natuurlijk persoon. Dit is niet alleen voor verantwoording, maar ook om mogelijke identiteitsdiefstal tegen te gaan.
Voorbeeld	
Mogelijke uitzondering	Voor test- en ontwikkelomgevingen kan van deze regel worden afgeweken, mits in de test- en ontwikkelomgeving geen productiedata wordt verwerkt.

IDnr	**IBB-TR05-LTB-R04**
BIO / NkBR verwijzing	BIO 9.3.1
Titel	Standaard (of default) accounts
Omschrijving	Standaard (default) accounts worden door leveranciers van informatiesystemen standaard meegeleverd. Voorbeeld is het standaard admin-account met wachtwoord "admin". Standaard (of default) accounts moeten worden disabled voor in gebruik name van een systeem of dienst. Tevens dienen alle standaardwachtwoorden te worden gewijzigd bij de eerste mogelijkheid, maar in ieder geval voordat het systeem of dienst in productie wordt genomen. Indien het gebruik van een standaard (of default) account noodzakelijk is voor de goede werking, dienen aanvullende beveiligingsmaatregelen te worden getroffen om misbruik van deze accounts te voorkomen. Ook dienen deze accounts aan een lijnmanager te worden toegewezen, die verantwoordelijk is voor de uitgifte, het gebruik en inname van deze accounts. Middels logging en monitoring dient het gebruik van deze accounts achteraf te worden beoordeeld.
Gerelateerde documenten	
Motivatie	Standaard (of default) accounts zijn bekend bij hackers en een eerste poging bij een aanval is om de wachtwoorden van standaard (of

	default) accounts te raden.
Voorbeeld	Een standaard (of default) 'root' of 'gast' account moet worden disabled of geheel worden verwijderd.
Mogelijke uitzondering	n.t.b.

IDnr	**IBB-TR05-LTB-R05**
BIO / NkBR verwijzing	BIO 9.4.2
Titel	Authenticatiemethode
Omschrijving	Indien de toegangsverlening plaatsvindt vanuit het eigen domein of gekoppelde vertrouwde zones, mogen de systemen gebruikers toegang verlenen op basis van gebruikersnaam en wachtwoord. Indien de toegangsverlening plaatsvindt vanaf het internet of een onvertrouwde zone, dienen de systemen gebruikers toegang te verlenen op basis van multi-factor authenticatie. De authenticatie methode moet herleidbaar zijn tot een unieke gebruiker en dient niet gekopieerd of verlopen te zijn binnen een korte tijdsperiode (e.g. 3 minuten). Naarmate de gevoeligheid van de gegevens hoger is, zijn meer beveiligingsmaatregelen nodig. Bijvoorbeeld aan het proces van uitgifte van een account (bijvoorbeeld een WID-controle[4]) en aan de authenticatie (bijvoorbeeld een twee-factor authenticatie tegen een wachtwoord in combinatie met een SMS-code of een pincode via een token). Naarmate de plaats van waaruit de gebruiker toegang wil krijgen minder betrouwbaar is, zijn er meer (beveiligings)maatregelen nodig. Bijvoorbeeld toegang vanaf een beveiligd netwerk van een ketenpartner of overheidsorganisatie is in de regel betrouwbaarder dan toegang 'van buiten af', zoals een internetcafé of vanaf een luchthaven.
Gerelateerde documenten	
Motivatie	Multi-factor authenticatie biedt betere bescherming.
Voorbeeld	Twee-factor-authenticatie (wachtwoord en token) is nodig om op afstand toegang te krijgen tot de digitale OM werkruimte en sessies moeten afgebroken worden na een vooraf gedefinieerde periode van inactiviteit.

[4] Bij een WID-controle wordt de identiteit vastgesteld. Voor het identificeren van een nieuwe medewerker wordt in deze gevallen een WID-scan gedaan waarbij men kopieën en scans van identiteitsbewijzen maakt en vastlegt.

Mogelijke uitzondering	n.t.b.

IDnr	**IBB-TR05-LTB-R06**
BIO / NkBR verwijzing	BIO 9.4.1.2
Titel	Toegang tot informatie en daarmee systemen is gebaseerd op het principe van Least Privilege
Omschrijving	Een gebruiker, in een bepaalde rol, dient alleen die informatie en systemen te kunnen benaderen die nodig is respectievelijk zijn voor het uitvoeren van zijn of haar taak in die rol.
Gerelateerde documenten	
Motivatie	Toegang tot systemen is gebaseerd op Least Privilege en is derhalve nooit ruimer dan strikt noodzakelijk voor de uitoefening van een functie. Dit is om misbruik en onopzettelijke schade tegen te gaan.
Voorbeeld	Least Privilege gaat over wat je mag doen binnen een systeem. Een administratief medewerker kan bijvoorbeeld aanpassingen doen in een document waarvan hij/zij eigenaar is. Gebruikers hebben slechts toegang tot de gegevens van een zaak indien zij rechtstreeks betrokken zijn bij de uitvoering van werkzaamheden ten behoeve van die zaak. Daarnaast hebben de beheerder en bewerker toegang, voor zover dit in het kader van beheer en bewerking noodzakelijk is.
Mogelijke uitzondering	n.t.b.

IDnr	**IBB-TR05-LTB-R07**
BIO / NkBR verwijzing	BIO 9.2.1, 9.2.2
Titel	Vaststellen en documenteren van autorisaties
Omschrijving	Autorisaties in een informatiesysteem dienen te worden ontworpen op basis van "Privacy- en Security-by-Design". Autorisaties worden vastgelegd in profielen. Dat doet de systeemeigenaar. Het bevoegd gezag kiest een autorisatieprofiel voor de betreffende medewerker. Autorisatieaanvragen worden door het bevoegde gezag of door een lijnmanager namens het bevoegd gezag ingediend bij de ICT-

	uitvoeringsorganisatie. Autorisatieaanvragen bevatten tenminste de volgende gegevens: naam aanvrager, gebruiker/begunstigde, aanvraagdatum, gewenste ingangsdatum, einddatum (bij tijdelijke medewerkers) en de gewenste bevoegdheden / autorisatieprofiel(en).
Gerelateerde documenten	"Beleid Logische Toegangsbeveiliging" IBD
Motivatie	Om op een gestandaardiseerde manier autorisaties in het systeem toe te kennen en het mogelijk te maken om periodiek te controleren op juistheid.
Voorbeeld	In de autorisatiematrix wordt vooraf vastgelegd welke autorisaties worden gekoppeld aan welke rollen
Mogelijke uitzondering	n.t.b.

IDnr	**IBB-TR05-LTB-R08**
BIO / NkBR verwijzing	BIO 9.2.2.1
Titel	Goedkeuring van autorisaties
Omschrijving	Een gemandateerd lijnmanager van het betreffende dienstonderdeel dient autorisatieverzoeken te beoordelen en is verantwoordelijk voor het genomen besluit. Het overdragen van deze verantwoordelijkheid gedurende afwezigheid mag enkel in de richting van een hoger geplaatste functionaris (opwaartse delegatie). Voor de autorisatieverzoeken, waarbij medewerkers toegang kunnen krijgen tot specifieke (of hoger gerubriceerde) informatie of gevoelige zaken (bijv. embargo onderzoeken) is de verantwoordelijke zaaksofficier degene die de autorisatieverzoeken beoordeelt.
Gerelateerde documenten	
Motivatie	Het besluit van een manager om een autorisatieverzoek toe te kennen vraagt kennis van processen en risico's. De lijnmanager is de eerste verdedigingslinie tegen beveiligingsrisico's. Per applicatie, systeem of netwerk-onderdeel kan het voorkomen dat er meer gemandateerden met dezelfde rol zijn voor het toekennen van autorisatieverzoeken.
Voorbeeld	De directeur keurt de autorisatieverzoeken van de afdelingshoofden goed. De afdelingshoofden keuren de autorisatieverzoeken van de medewerkers goed. Bij afwezigheid van een afdelingshoofd keurt de directeur de autorisatieverzoeken van een medewerker goed.

Mogelijke uitzondering	n.t.b.

IDnr	**IBB-TR05-LTB-R09**
BIO / NkBR verwijzing	BIO 9.2.6
Titel	Verantwoordelijkheid voor autorisaties externe partijen
Omschrijving	Het toekennen en controleren van persoons- en systeemaccounts voor OM-systemen in gebruik van externe partijen dient gedaan te worden door de partij binnen het OM die verantwoordelijk is voor de uitbesteding
Gerelateerde documenten	
Motivatie	De verantwoordelijke voor de uitbesteding heeft zicht op de kaders rondom de te verrichten werkzaamheden en kan deze vertalen richting contract, autorisaties en uitvoerende medewerkers
Voorbeeld	De organisatie laat de salarisverwerking doen door een 3e partij, waarbij zaken als geheimhouding, "need-to-know" van personeelsgegevens door de verantwoordelijke worden vastgelegd in het contract met de 3e partij.
Mogelijke uitzondering	n.t.b.

IDnr	**IBB-TR05-LTB-R10**
BIO / NkBR verwijzing	BIO 9.2.2
Titel	Registratie van autorisatiebesluiten
Omschrijving	Ieder(e) applicatie, systeem, en netwerk onderdeel dient een geactualiseerde administratie bij te houden van geautoriseerde accounts, wie de autorisatie toegekend heeft (manager en tweede persoon met autorisatie bevoegdheid) en wanneer.
Gerelateerde documenten	
Motivatie	Voor alle bestaande accounts en autorisaties moet herleid kunnen worden wie de verzoeken heeft goedgekeurd en wanneer, daarom moet een register bijgehouden worden.
Voorbeeld	Excel lijst met goedkeuringen van managers en controleurs.
Mogelijke uitzondering	n.t.b.

IDnr	IBB-TR05-LTB-R11
BIO / NkBR verwijzing	BIO 9.2.5.1
Titel	Juistheid van toegekende autorisaties
Omschrijving	Minstens eenmaal per half jaar dient de autorisatiebevoegdheid van iedere werknemer getoetst te worden om te controleren of de autorisatie passend is voor de huidige functie (manager controleert).
Gerelateerde documenten	
Motivatie	Autorisatie bevoegdheid kan veranderen. Onvoldoende autorisatie zal snel opgemerkt worden, onnodig ruime autorisatie wordt minder snel opgemerkt.
Voorbeeld	Vanwege veranderende processen of een wissel in functieomschrijving van een werknemer blijken bepaalde autorisaties overbodig.
Mogelijke uitzondering	n.t.b.

IDnr	IBB-TR05-LTB-R12
BIO / NkBR verwijzing	BIO 9.2.6
Titel	Functiewijziging van de gebruiker
Omschrijving	Bij verandering van functie, opgedragen taken of reorganisatie dient het gemandateerd afdelingshoofd en/of de zaaksofficier de autorisaties betrekking hebbend op de functie in te trekken, voordat de medewerker de functie verlaat.
Gerelateerde documenten	
Motivatie	De manager zorgt ervoor dat autorisatiebevoegdheden van vertrekkende medewerkers niet misbruikt worden.
Voorbeeld	Een voormalig HR medewerker die nu werkt bij Beheer dient geen toegang meer te hebben tot alle HR gerelateerde werkdocumenten.
Mogelijke uitzondering	n.t.b.

IDnr	IBB-TR05-LTB-R13
BIO / NkBR verwijzing	-
Titel	Niet actief gebruikte accounts
Omschrijving	Wanneer een gebruikersaccount niet meer wordt gebruikt, dient deze na 42 dagen op disabled gezet te worden. De lijnmanager van de medewerker wordt geïnformeerd over het disablen van accounts en dient deze te controleren. Na akkoord van een manager dat een account langer geldig blijft, worden de overige accounts na 180 dagen verwijderd.
Gerelateerde documenten	Opstellen procedure gebruikersbeheer door DVOM
Motivatie	Als een account niet langer gebruikt wordt door de originele gebruiker kan deze onopgemerkt misbruikt worden voor toegang door onbevoegden.
Voorbeeld	Een medewerker is langdurig ziek, waardoor de periode van 42 of 180 dagen wordt overschreden. Dit account dient dan disabled te worden door een opdracht van de manager of automatisch na 42 dagen. Dit account hoeft niet verwijderd te worden, mits akkoord van de bevoegd lijnmanager.
Mogelijke uitzondering	Functionele mailgroepen die alleen worden gebruikt om mail te ontvangen en waarop niet wordt ingelogd. Voor kernapplicaties kan met onderbouwing afgeweken worden van de 42-dagen regel en 180-dagen regel.

IDnr	IBB-TR05-LTB-R13.1
BIO / NkBR verwijzing	-
Titel	Verwijderen accounts bij beëindigen dienstverband
Omschrijving	Wanneer een gebruiker zijn/haar dienstverband gaat beëindigen, informeert de lijnmanager de ICT-uitvoeringsorganisatie dat de medewerker uit dienst gaat inclusief ingangsdatum. Hierbij geeft de lijnmanager naast het gebruikte netwerkaccount ook de aan dit account gerelateerde applicatieaccounts op. Vanuit de centrale registratie wordt een automatisch signaal doorgegeven waarmee het netwerkaccount wordt geblokkeerd. De ICT-uitvoeringsorganisatie blokkeert vervolgens de applicatieaccounts van het geblokkeerde netwerkaccount.

Gerelateerde documenten	Opstellen procedure gebruikersbeheer door DVOM
Motivatie	De applicatieaccounts zijn niet altijd gekoppeld aan netwerkaccounts. Doordat de lijnmanager vooraf een opgave dient te verstrekken aan de ICT-uitvoeringsorganisatie, is het OM in staat om inzicht te krijgen in alle gebruikte applicatieaccounts van een gebruiker.
Voorbeeld	
Mogelijke uitzondering	n.t.b.

IDnr	**IBB-TR05-LTB-R14**
BIO / NkBR verwijzing	BIO 12.4.1
Titel	Loggen van relevante gebruikershandelingen of -activiteiten
Omschrijving	Van iedere inlogpoging voor een applicatie, systeem en netwerkonderdeel, alsmede handelingen of gebeurtenissen die een controlespoor vereisen, dient een log aangemaakt en bijgehouden te worden. De activiteiten van functioneel accounts dienen te worden gelogd volgens het reguliere proces.
Gerelateerde documenten	Logging en Monitoring
Motivatie	Nodig om ongeautoriseerde toegangspogingen te herkennen (login logging) alsmede het opmerken van kwaadaardige intenties (audit log)
Voorbeeld	Wanneer iemand op het netwerk inlogt wordt hiervoor een log aangemaakt
Mogelijke uitzondering	n.v.t.

IDnr	**IBB-TR05-LTB-R15**
BIO / NkBR verwijzing	BIO 9.4.2.2
Titel	Externe accounts
Omschrijving	Voor het verlenen van toegang tot het netwerk door externe partijen (leveranciers) wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden de leveranciers toegang (kunnen) krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend. De in dit beleid gestelde eisen ten aanzien van interne OM accounts, zijn onverkort van toepassing voor externe accounts.

	We onderscheiden 3 groepen externe partijen 1. Medewerkers van externe vertrouwde partijen: Bijvoorbeeld Rechtspraak (ZM), Nationale Politie (NP) 2. Medewerkers van leveranciers van het OM (ICT diensten): Bijvoorbeeld Atos, Fujitsu, Axians, ODC-Noord 3. Medewerkers van overige externe partijen: Bijvoorbeeld CJIB, Justis, COVOG, IT-auditors zoals ADR en KPMG, pentesters en wetenschappelijke onderzoekers
Gerelateerde documenten	
Motivatie	Gezien de grote verschillen tussen externe partijen verschillen ook de voorwaarden onder welke de partijen toegang krijgen.
Voorbeeld	Een rechter-commissaris dient niet nogmaals een VOG te laten zien, terwijl dit wel gevraagd wordt van medewerkers van externe leveranciers (ICT middelen).
Mogelijke uitzondering	n.t.b.

IDnr	**IBB-TR05-LTB-R16a**
BIO / NkBR verwijzing	BIO 9.2.3
Titel	Accounts met speciale of hoge bevoegdheden
Omschrijving	Het toekennen van accounts met speciale of hoge bevoegdheden aan medewerkers, veelal technische beheerders en ontwikkelaars, vindt plaats door deze medewerkers een extra "beheer" account te geven naast hun gewone gebruikersaccount. Het aanmaken en de uitgifte van deze "beheer" accounts wordt met specifieke maatregelen beveiligd, waarbij een directe controle plaatsvindt op het aanmaken van zo'n "beheer" account door middel van functiescheiding. De aangemaakte "beheer" accounts worden minimaal ieder kwartaal beoordeeld op noodzaak.
Gerelateerde documenten	
Motivatie	Met hoge rechten kan een gebruiker activiteiten uitvoeren op IT-systemen die zonder extra maatregelen kunnen ingrijpen op de integriteit van het systeem en het toegang verkrijgen tot vertrouwelijke data. Accounts met speciale of hoge bevoegdheden brengen een groter risico met zich mee, derhalve dienen deze accounts bij uitgifte gecontroleerd te worden met behulp van

	functiescheiding en gedurende het gebruik vaker te worden beoordeeld op noodzakelijkheid.
Voorbeeld	Voorbeelden van groepen met speciale bevoegdheden zijn beheerders, ontwikkelaars en pentesters
Mogelijke uitzondering	n.t.b.

IDnr	**IBB-TR05-LTB-R16b**
BIO / NkBR verwijzing	BIO 9.2.3
Titel	Speciale bevoegdheden
Omschrijving	Het toekennen van speciale bevoegdheden (autorisaties of permissies) aan medewerkers, veelal technische beheerders en ontwikkelaars, die bevoegd zijn om o.a. speciale of beheer tools te gebruiken vindt terughoudend plaats. Het gebruik van deze speciale bevoegdheden (autorisaties of permissies) wordt door logging afzonderlijk vastgelegd (zie beleid logging). De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.
Gerelateerde documenten	
Motivatie	Speciale bevoegdheden brengen een groter risico met zich mee, derhalve dienen deze vaker beoordeeld te worden.
Voorbeeld	Voorbeelden van groepen met speciale bevoegdheden zijn beheerders, ontwikkelaars en pentesters
Mogelijke uitzondering	n.t.b.

Bladzijde 77 t/m 113 - BR

[redacted]

IDnr	**IBB-TU-HBO-01**
BIO / NkBR verwijzing	BIO 9.2
Titel	Beheer van toegangsrechten van gebruikers
Omschrijving	Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen. Dep.V.: Toegangsrechten van gebruikers worden periodiek, minimaal jaarlijks, geëvalueerd. Het interval is beschreven in het toegangsbeleid en is bepaald op basis van het risiconiveau. Stg.C: Toegangsrechten van gebruikers worden periodiek, minimaal eens per 3 maanden geëvalueerd. Het interval is beschreven in het toegangsbeleid en is bepaald op basis van het risiconiveau. Stg.G: Toegangsrechten van gebruikers worden periodiek, minimaal eens per maand, geëvalueerd. Het interval is beschreven in het toegangsbeleid en is bepaald op basis van het risiconiveau.
Gerelateerde documenten	ntb
Motivering	
Voorbeeld	ntb
Mogelijke uitzondering	ntb

BR

[redacted]

Bladzijde 115 t/m 137 - BR