POLITIE

Beleidskader logging

5.1.2.e

Definitief

Versie 1.0

Versie datum 1 mei 2018

Rubricering Klik hier om rubricering in te voeren.

«waakzaam en dienstbaar»

Documentinformatie

Distributie

Versie	Verzend datum	Naam	Afdeling / Functie
0.1	21-09-2017	5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e	Directie IV, PPI, VIK
0.2	02-11-2017	5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e	Directie IV, Dienst ICT, Dienst IM, VIK, FDO, Midden Nederland
0.3	06-12-2017	5.1.2.e , 5.1.2.e , 5.1.2.e	Directie IV
0.4	11-12-2017	BBVO, COR	
0.4	06-03-2018	KMTO	
0.5	29-03-2018	Dick Heerschop	CIO
1.0	01-05-2018	Vastgesteld door Dick Heerschop	CIO

Inhoudsopgave

Documentinformatie 2

Inhoudsopgave 2

Inleiding 4

1. Juridisch kader 5
   1.1 Logging op grond van de AVG en de Wpg 5
   1.2 Logging op grond van de Wpg 5
   1.3 Wettelijk regime loggegevens 6
   1.4 Instemmingsrecht ondernemingsraad 6

2. Uitwerking relevante aspecten 6
   2.1 Voor welke doelen wordt gelogd? 6
   2.2 In welke gevallen en hoe mogen de gegevens gebruikt worden? 7
   2.3 Wie moeten toegang tot de logging hebben? 7
   2.4 Welke gegevens moeten worden gelogd? 8
   2.5 Wat zijn de bewaartermijnen van logging? 9
   2.6 Verantwoordelijkheid ten aanzien van de loggingsdata 9

Bijlage – relevante artikelen 10

Inleiding

Dit kader maakt duidelijk waarmee bij de ontwikkeling en het gebruik van loggingtoepassingen rekening moet worden gehouden. Alle ontwikkelingen dienen te passen binnen het hier geschetste kader en de gestelde doelen mogelijk te maken. Daarbij is er het streven om de huidige ontwikkelingen op het gebied van logging op elkaar af te stemmen en een eenduidige loggingssystematiek te hanteren

Daarbij is relevant dat er per 6 mei 2018 extra verplichtingen op de politie afkomen als gevolg van de voorgenomen wijzigingen van de Wet politiegegevens (Wpg) ter implementatie van de Europese Richtlijn gegevensbescherming opsporing en vervolging (richtlijn). Eén van die verplichtingen ziet op logging van bepaalde verwerkingen van politiegegevens.

Ook ten aanzien van persoonsgegevens die niet in het kader van de uitvoering van de politietaak worden verwerkt, maar bijvoorbeeld in de bedrijfsvoering, gaan vanaf 25 mei 2018 als gevolg van de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) nieuwe verplichtingen gelden. Hoewel de AVG, in tegenstelling tot de Wpg, geen specifieke loggingsverplichting kent, komt ook daar de nadruk op verantwoording en documentatie te liggen. Logging is een middel om invulling te geven aan de plicht om passende technische en organisatorische maatregelen te treffen zodat persoonsgegevens op een dusdanige manier worden verwerkt dat een passende beveiliging gewaarborgd is. Bovendien is het een noodzakelijke maatregel om verantwoording af te kunnen leggen over ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of betrouwbaarheid (“integriteit en vertrouwelijkheid”)[1].

Dit kader geldt voor alle loggingsmechanismen, waaronder die op Wpg-verwerkingen en AVG-verwerkingen.
Ten eerste wordt het juridisch kader rond logging geschetst. Omdat dit juridisch kader ruimte biedt voor interpretatie, wordt vervolgens aan de hand van zes vragen uiteengezet op welke manier daar invulling aan wordt gegeven. Het gaat daarbij om de volgende aspecten:

1) Voor welke doelen wordt gelogd?
2) In welke gevallen en onder welke voorwaarden mogen de loggegevens gebruikt worden?
3) Wie moeten (en mogen) toegang tot de loggegevens hebben?
4) Welke gegevens moeten worden gelogd?
5) Wat zijn de bewaartermijnen van loggegevens?
6) Wie heeft de verantwoordelijkheid ten aanzien van de loggingsdata?

Aan de hand van dit beleidskader wordt inzichtelijk met welke eisen bij onder andere de ontwikkeling van een generiek loggingplatform, de ontwikkeling van een applicatie, en het vormgeven van toegang tot de logging, rekening moet worden gehouden.

De eisen zijn primair opgesteld voor de productieomgevingen, maar zijn ook van toepassing op ontwikkel-, test-, acceptatie- en opleidingsomgevingen.

[1] Artikel 5, lid 1, onder f van de AVG.

1. Juridisch kader

1.1 Logging op grond van de AVG en de Wpg

Zowel de AVG als de Wpg stelt strenge eisen aan de beveiliging van persoonsgegevens en aan de manier waarop hierover verantwoording moet worden afgelegd. Daar waar passende technische en organisatorische maatregelen moeten worden genomen zodat een passende beveiliging gewaarborgd is, moet onder meer gedacht worden aan:

- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen[2];
- te waarborgen en te kunnen aantonen dat de verwerking van politiegegevens wordt verricht in overeenstemming met hetgeen bij of krachtens deze wet is bepaald[3].

Daarnaast moeten in het kader van de meldplicht datalekken[4] bij een inbreuk op de beveiliging van persoonsgegevens de waarschijnlijke gevolgen van de inbreuk te bepalen zijn.

Logging wordt door de Autoriteit Persoonsgegevens (AP) aangemerkt als één van de technische maatregelen die in dit verband genomen moet worden.

Zoals in de inleiding vermeld is er geen bepaling in de AVG die voorschrijft welke handelingen gelogd moeten worden en voor welk doel de vastgelegde gegevens gebruikt mogen worden. De Wpg kent wel zo'n bepaling.

1.2 Logging op grond van de Wpg

Naast de algemene verplichting om passende technische en organisatorische maatregelen te nemen zodat een passende beveiliging gewaarborgd is, kent het (concept)wetsvoorstel voor de Wpg een specifieke bepaling over logging. Uit de huidige tekst van artikel 32a Wpg[5] volgt dat gezorgd moet worden voor logging van ten minste de volgende verwerkingen van politiegegevens[6] in geautomatiseerde systemen:

- verzameling;
- wijziging;
- raadpleging;
- verstrekking onder meer in de vorm van doorgiften;
- combinatie;
- vernietiging.

Daarbij moet de identificatie van de persoon die de persoonsgegevens heeft geraadpleegd of bekend heeft gemaakt worden geregistreerd. Aangevuld met de datum en het tijdstip van handelen en zo mogelijk de identiteit van de ontvangers (bij verstrekken en doorgiften). Op basis daarvan moeten de redenen voor de verwerkingsactiviteiten kunnen worden vastgesteld.[7]

De vastgelegde gegevens worden uitsluitend gebruikt voor:

1. de controle van de rechtmatigheid van de gegevensverwerking;
2. interne controles;
3. ter waarborging van de integriteit en de beveiliging van de politiegegevens;
4. strafrechtelijke procedures.

Bij dit artikel is geen uitgebreide toelichting opgenomen. Alleen ten aanzien van het laatstgenoemde doel wordt toegelicht dat gedacht kan worden aan strafvervolging op grond van ambtelijke corruptie, waarbij de gelogde gegevens kunnen worden gebruikt om aan te tonen dat een persoon op een bepaald tijdstip in het systeem gegevens heeft geraadpleegd, gewijzigd of gewist.

---

[2] Artikel 5, lid 1, onder f AVG en artikel 32 AVG.
[3] Artikel 4a, lid 1, onder a Wpg.
[4] Artikel 33 en 34 AVG en artikel 33a Wpg.
[5] De concepttekst van art. 32a Wpg is als bijlage opgenomen.
[6] Een politiegegeven is elk persoonsgegeven dat in het kader van de uitoefening van de politietaak wordt verwerkt (artikel 1, onder a Wpg).
[7] Overweging 57 bij de Richtlijn gegevensbescherming opsporing en vervolging.

1.3 Wettelijk regime loggegevens

Uit bovenstaande volgt dat de logging tot doel heeft interne controles mogelijk te maken, de integriteit en de beveiliging van de politiegegevens te waarborgen en strafrechtelijke procedures te kunnen voeren. Deze doelen staan los van de uitvoering van de politietaak. Voor zover de logging persoonsgegevens bevat, vallen deze dan ook niet onder de werking van de Wpg, maar onder de werking van de AVG.

1.4 Instemmingsrecht ondernemingsraad

De ondernemingsraad heeft instemmingsrecht voor elk voorgenomen besluit tot vaststelling, wijziging of intrekking van een regeling inzake voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de in de onderneming werkzame personen.[8] Dit geldt dus zowel voor verwerkingen die onder de Wpg als onder de AVG vallen. Zoals in de inleiding al is aangegeven, is logging in het kader van de Wpg een wettelijke verplichting en is logging in het kader van de AVG een manier om te voldoen aan de verantwoordingsplicht. Het instemmingsrecht ten aanzien van de Wpg zal dus beperkter zijn en vooral zien op de wijze waarop invulling wordt gegeven aan de wettelijke verplichting.
Indien de ondernemingsraad heeft ingestemd met dit beleidsvoorschrift moet overeenkomstig hetgeen hierin bepaald is gewerkt worden. Wanneer bij de ontwikkeling van nieuwe logtoepassingen behoefte is aan een afwijkende invulling, met name ten aanzien van de vast te leggen gegevens of het gebruik daarvan, dan is dat opnieuw instemmingsplichtig.

2. Uitwerking relevante aspecten

Zoals bij het juridisch kader al is vermeld geeft de toelichting bij het loggingsartikel uit de Wpg geen nadere uitleg bij de doelen waarvoor de vastgelegde gegevens gebruikt mogen worden. Om daar duidelijkheid over te bieden wordt in dit voorschrift bepaald op welke wijze aan deze verplichting, en die van de AVG, invulling wordt gegeven.

2.1 Voor welke doelen wordt gelogd?

Loggingsfunctionaliteit wordt al jaren gebruikt binnen de politie, maar de wijze van logging verschilt per applicatie en de loggegevens worden gebruikt voor verschillende doeleinden. In onderstaande tabel wordt inzichtelijk gemaakt voor welke doelen al gelogd wordt en of deze overeenkomen met één (of meer) van de vier mogelijkheden die het juridisch kader biedt (zie paragraaf 1.2):

	Bestaande doelen van logging	**Conform juridisch kader?**
a)	Voor beveiligingsdoeleinden en ten behoeve van VIK-onderzoek achteraf. Gedacht kan worden aan hackers, mollen etc.	(1)controle van de rechtmatigheid van de gegevensverwerking.
		(2) interne controles.
		(3) waarborging integriteit en beveiliging van politiegegevens.
		(4) strafrechtelijke procedures.
b)	Technisch herstel naar een (eerdere) integere situatie, ter waarborging van de integriteit, beveiliging en beschikbaarheid van de politiegegevens.	(3) waarborging integriteit en beveiliging van politiegegevens.
c)	Informeren van betrokkene en de Autoriteit Persoonsgegevens in geval van een datalek in het kader van de meldplicht datalekken.	(1) controle van de rechtmatigheid van de gegevens verwerking.
d)	Ter informatie aan de burger of de medewerker bij een verzoek om kennisneming in het kader van ‘rechten van betrokkene’. Daarbij moet ook meegedeeld worden aan wie gegevens zijn verstrekt. De medewerker heeft daarbij ook recht op kennisneming van de logbestanden die op hem betrekking hebben (bijv. ten behoeve van een VIK-onderzoek).	(1) controle van de rechtmatigheid van de gegevens.
e)	Operationeel gebruik: eerdere handelingen op het systeem kunnen bijdragen aan opsporingsonderzoeken (bijv. zoekacties).	(4) strafrechtelijke procedures

[8] Artikel 27, lid 1, onder l van de Wet op de Ondernemingsraden

Atypische signalen[9]

Naast deze bestaande doeleinden van logging is het noodzakelijk om met behulp van geautomatiseerde tools naar atypische signalen te zoeken en op die manier mogelijk onrechtmatig gebruik real time te detecteren. Dit is een effectieve maatregel die ons op het spoor kan zetten van technische bedreigingen van buitenaf die door de eerste beveiligingslagen heen zijn gedrongen, of misbruik van binnenuit dat met de gebruikelijke middelen soms onder de radar blijft. De aanleiding om hiermee te starten ligt in toenemende dreiging, toename van consequenties van een inbreuk door centralisatie en de onmogelijkheid 'derden' altijd buiten te houden[10].

Door middel van een gecontroleerde pilot wordt een zorgvuldige werkwijze ontwikkeld die ernstig misbruik en bedreigingen bestrijdt, zonder het belang van de medewerkers uit het oog te verliezen. De uitwerking van deze pilot en het voorgenomen beleid is uitgebreid beschreven in het document *Atypische signalen,* waarbij rekening is gehouden met de kaders van het onderhavige beleidsvoorschrift.

Alle bovengenoemde doeleinden van logging, waaronder het genereren van real time signalen van mogelijk atypisch gebruik, vallen binnen de mogelijkheden die de Wpg biedt.

2.2 In welke gevallen en hoe mogen de gegevens gebruikt worden?

De vastgelegde gegevens mogen uitsluitend gebruikt worden ten behoeve van de eerder genoemde doelen. Bij strafrechtelijke procedures kan, gelet op de toelichting, gedacht worden aan onderzoeken met betrekking tot ambtelijke corruptie. Het is echter de vraag hoe ruim 'strafrechtelijke procedures' geïnterpreteerd kan worden en op welke manier operationeel gebruik van loggegevens vormgegeven kan worden. In de eenheid Midden Nederland is onderzocht op welke wijze loggingdata van smartphones van politiemedewerkers op structurele wijze kunnen worden gebruikt ten behoeve van de opsporing. Deze voorstellen moeten in een afzonderlijk traject nader beoordeeld worden.

Bij het ontwerp van de loggingsfaciliteiten moeten maatregelen worden genomen waardoor dit zo goed mogelijk ondersteund wordt (privacy & security by design). Daarbij moet gedacht worden aan:

- Hanteren van een gelaagd model: afhankelijk van het doel van de gebruiker van de logging moeten de loggegevens worden aangeboden.
- De loggegevens moeten zo specifiek mogelijk worden aangeboden: geen onevenredige belasting van de systemen en zo min mogelijk inbreuk op de bescherming van de persoonlijke levenssfeer.
- Vastlegging van de bewaartermijnen in de logging (dedicated applicaties). Of in ieder geval metadata waaruit de bewaartermijn van de loggegevens kan worden afgeleid.

2.3 Wie moeten toegang tot de logging hebben?

In onderstaande tabel is uitgewerkt welke personen/afdelingen/instanties direct of indirect toegang moeten krijgen tot de loggegevens voor zover zij deze nodig hebben voor de uitvoering van hun taken. De toegang tot de logging kan op persoon worden georganiseerd (bijv. bij VIK) of via tooling (ATL), of via beide (bijv. SOC). De tabel geeft dus een nadere uitwerking van paragraaf 2.1 en 2.2.

Wie?	Waarom?	Waarvoor?
Security Operations Centre (SOC)	Bewaakt de ICT-infrastructuur van de politie tegen in- en externe bedreigingen. Cybersecurity management.	Voor beveiligingsdoeleinden moet rechtstreeks in logging gezocht kunnen worden naar voorkomen van malware, atypische signalen, virussen, etc. Daarnaast is het nodig dat de audittrail kan worden vastgesteld.
Functioneel en technisch beheerders	Op operationeel respectievelijk technisch niveau verantwoordelijk voor continuïteit en aansturing van de informatievoorziening.	Uitsluitend tot de logging van de eigen systemen en applicaties. Ten behoeve van het technisch herstel naar een eerdere integere situatie, ter waarborging van de integriteit, beveiliging en beschikbaarheid van politiegegevens op aangeven van anderen. Bijv. een persoon die verzoekt om herstel van een eigen map of

[9] Onderstaande tekst sluit aan bij het document Atypisch dat separaat in besluitvorming wordt gebracht.

[10] Vanzelf blijven we inspanning leveren 'derden' tegen te houden, echter wordt wereldwijd erkend dat alleen tegenhouden geen oplossing meer is omdat er altijd onvolkomenheden zijn in bijvoorbeeld software en netwerkinrichting (denk aan zero days).

		een eigenaar van een database voor de gehele database.
Forensisch Digitale Opsporing (VIK)	Genereert de daadwerkelijke loggegevens in een leesbaar bestand.	Ten behoeve van verstrekking aan VIK en binnen uit te werken kaders voor operationele doeleinden (al dan niet op vordering).
CISO/ Specialist Cybersecurity	Heeft een rol bij beveiligingsincidenten en in het kader van de meldplicht datalekken.	Voor beveiligingsdoeleinden is het nodig dat de audittrail kan worden vastgesteld. In het kader van de meldplicht datalekken is het nodig dat inzichtelijk wordt welke gevolgen de inbreuk op de beveiliging van persoonsgegevens voor een betrokkene heeft.
Veiligheid, Integriteit en Klachten (VIK)	Voert oriënterende, disciplinaire en strafrechtelijke onderzoeken uit.	Ten behoeve van een VIK-onderzoek kan het noodzakelijk zijn de gedragingen van medewerkers vast te stellen en in het onderzoek te betrekken.
Autoriteit Persoonsgegevens (AP)	Toezichthouder ogv art. 57 en 58 AVG en art. 35a en 35b Wpg	Ten behoeve van de vervulling van zijn toezichthoudende taken (art. 58, lid 1, onder e AVG en art. 35b jo art. 6a, lid 3 Wpg)
Functionaris voor de gegevensbescherming (FG)	Toezichthouder ogv art. 38 en 39 AVG en art. 36 Wpg.	Ten behoeve van de vervulling van zijn toezichthoudende taken (art. 38, lid 2 AVG en art. 36 jo 6a, lid 3 Wpg).
Privacyfunctionaris	Ziet namens de verwerkingsverantwoordelijke toe op de naleving van de Wpg (art. 34 Wpg)	Ten behoeve van de vervulling van zijn toezichthoudende taken (art. 34 jo art. 6a, lid 3 Wpg)
In- / en externe auditor	Voert in opdracht van de verwerkingsverantwoordelijke interne respectievelijk externe privacy audits uit (art. 33 Wpg).	Ten behoeve van de vervulling van zijn audittaken (art. 33 jo art. 6a, lid 3 Wpg).
Privacydesk ivm rechten van betrokkene	Behandelt verzoeken van burgers of medewerkers in het kader van het recht op kennisneming.	Ten behoeve van de behandeling van verzoeken om kennisneming is het nodig te weten welke politiegegevens de voorgaande vier jaren verstrekt zijn en wie de ontvanger van die gegevens is.

De manier waarop de toegang verleend wordt, bij wie de verantwoordelijkheden zijn belegd, hoe de toegang kan worden aangevraagd, onder welke voorwaarden de toegang verleend wordt etc. moet nader worden uitgewerkt. Daarbij is het relevant te vermelden dat de condities uit het reguliere proces worden gevolgd. Dit betekent bijvoorbeeld dat daar waar ‘heimelijken’ in het primaire proces worden afgeschermd, deze ook in de loggegegevens worden afgeschermd. Als ‘heimelijken’ in het primaire proces niet worden afgeschermd is het niet mogelijk dit in de loggegevens wel te organiseren.

2.4 Welke gegevens moeten worden gelogd?

Uitgangspunt is dat logging de registratie in het systeem aanvult waardoor de audittrail (“begin-einde”) kan worden vastgesteld. Daarbij moet rekening worden gehouden met het verschil tussen logging en journaling. Dit betekent dat systemen de historische antwoorden op zoekvragen weliswaar moeten kunnen reproduceren, maar dat dit, om de loggingfunctionaliteit niet te zwaar te belasten, idealiter via journaling in het systeem gerealiseerd wordt. Hetzelfde geldt voor de gegevens die nodig zijn om de authenciteit en de integriteit van informatie te kunnen vaststellen.

Kijkend naar de wettelijke eisen, maar ook naar de behoefte van de organisatie, moeten de volgende gegevens gelogd worden:

1. De handeling (in veel gevallen de zoekvraag).
2. De resultaten van de zoekvraag. Bij voorkeur worden deze resultaten niet via de logging vastgelegd, maar kunnen deze via de opslag van het systeem gereproduceerd worden.
3. De vervolgvragen (doorklikken). Bij een zoekvraag in analysetools zoals Palantir is het niet nodig alle resultaten te behouden, maar als de onderzoeker doorklikt op bijvoorbeeld een kenteken moet dat wel gelogd worden.

4. De identiteit van de (natuurlijke) persoon die de handeling verricht. Dit kan aan de hand van accountgegevens, eventueel ondersteund door IP-adres, IMEI, locatie (evt. via GPS), tijdstip of een combinatie daarvan. Bij de inrichting daarvan moet een afweging plaatsvinden over de noodzakelijkheid.
5. Het tijdstip van het handelen en zo mogelijk de identiteit van de ontvangers.
6. Technische transacties (wie heeft wanneer toegang tot applicaties, maar ook gebouwen). Deze gegevens vallen grotendeels onder de werking van de AVG.
7. Gebruikershandelingen (adhv CRUD-principe: Create, Read, Update & Delete).

Voor zover gebruik wordt gemaakt van de loggegevens, moeten deze handelingen vastgelegd worden zodat daar verantwoording over kan worden afgelegd.

2.5 Wat zijn de bewaartermijnen van logging?

In de Memorie van Toelichting bij art. 32a Wpg staat dat de verwerkingsverantwoordelijke (de korpschef) de bewaartermijn voor de gelogde gegevens dient vast te stellen in overeenstemming met de AVG. Vervolgens wordt gesteld dat het in de rede ligt de bewaartermijn te koppelen aan de periodieke privacy audits. Voor deze audits geldt een termijn van vier jaar.[11] Daarna kan nog een hercontrole plaatsvinden.
De (maximale) termijn van vijf jaar is voor de onder 2.1 genoemde doelen werkbaar.

Benadrukt moet worden dat de bewaartermijn van loggingsgegevens in het kader van de AVG, met name de bedrijfsvoeringsapplicaties, op basis van een risico-inschatting lager kan uitvallen. Als voorbeeld kan de logging van het zaalreserveringssysteem worden genoemd.
Bovendien moeten gegevens die nodig zijn om de authenciteit en integriteit van informatie vast te kunnen stellen net zolang bewaard blijven als de informatie zelf. Het is echter niet nodig dat deze gegevens ook tot personen (medewerkers) herleidbaar zijn.

2.6 Verantwoordelijkheid ten aanzien van de loggingsdata

Uit het beleidskader *Verantwoordelijkheid voor gegevens*[12] is af te leiden wie verantwoordelijk is voor de loggingsdata.

Aangezien het in dit geval om een korpsbrede voorziening gaat en er dus geen procesverantwoordelijke is aan te wijzen, volgt hieruit dat de Gegevensautoriteit (GA) eigenaar is van de dataset en daar verantwoordelijkheid voor heeft. De GA is niet verantwoordelijk voor het daadwerkelijk gebruik van de loggegevens of de ondersteunende tooling.

[11] Artikel 6:5, eerste lid van het Besluit politiegegevens
[12] Raadpleegbaar via de Agorasite van de GA

Bijlage – relevante artikelen

Onderstaande tekst is onder voorbehoud. Het wetsvoorstel ligt bij de Raad van State.

Artikel 32. (documentatie)

1. De verwerkingsverantwoordelijke draagt zorg voor de schriftelijke vastlegging van:
   a) de doelen van de onderzoeken, bedoeld in artikel 9, tweede lid;
   b) de verstrekking of doorgifte van politiegegevens op grond van paragraaf 3, met uitzondering van de verstrekking, bedoeld in artikel 17 en artikel 24, eerste en tweede lid, indien dit zich niet verdraagt met het belang van de veiligheid van de staat;
   c) de feitelijke of juridische redenen die ten grondslag liggen aan een afwijzing, bedoeld in artikel 27, eerste lid;
   d) een inbreuk op de beveiliging van persoonsgegevens, bedoeld in artikel 33a, inclusief de feiten omtrent de inbreuk, de gevolgen ervan en de maatregelen die zijn getroffen ter correctie.
2. Bij de doorgifte van politiegegevens aan een verwerkingsverantwoordelijke in een derde land of aan een internationale organisatie, bedoeld in artikel 17b, tweede lid, onderdeel b, en derde lid, omvat de schriftelijke vastlegging de datum en tijd van doorgifte, informatie over de ontvangende bevoegde autoriteit, de reden van doorgifte en de doorgegeven gegevens zelf.
3. De verantwoordelijke draagt zorg voor de schriftelijke melding van een gemeenschappelijke verwerking van politiegegevens aan de Autoriteit persoonsgegevens.
4. De politiegegevens, bedoeld in het eerste lid, worden bewaard tenminste tot de datum waarop de laatste controle, bedoeld in artikel 33, is verricht.
5. Bij of krachtens algemene maatregel van bestuur worden nadere regels gesteld over de wijze van vastlegging.

Memorie van Toelichting - artikel 32 (documentatie)

Eerste lid

De wet kent thans een zogenaamde protocolplicht, dat wil zeggen dat bepaalde gegevensverwerkingen schriftelijk vastgelegd moeten worden. Anders dan de registerplicht, heeft de protocolplicht betrekking op afzonderlijke verwerkingsactiviteiten in een specifiek geval. De richtlijn schrijft documentatie, dat wil zeggen schriftelijke vastlegging, voor van bepaalde verwerkingsactiviteiten. Het begrip 'schriftelijk' heeft betrekking op de vastlegging door middel van schrifttekens, hieronder valt ook de vastlegging in elektronische vorm.
De verplichtingen van de richtlijn vormen aanleiding tot aanpassing c.q. aanvulling van dit lid. De verplichting tot vastlegging van de gegevens die op grond van het bepaalde bij of krachtens artikel 13, vierde lid, worden vastgelegd, in onderdeel b van dit lid, is geschrapt omdat deze verplichting aldaar reeds is geregeld. De vastlegging van de toekenning van de autorisaties wordt overgeheveld naar het voorgestelde artikel 31, omdat deze geen betrekking heeft op afzonderlijke verwerkingsactiviteiten in een specifiek geval. De vastlegging van de geautomatiseerde vergelijking of het in combinatie met elkaar verwerken van politiegegevens is geschrapt omdat deze vastlegging reeds onder de verplichting tot het langs elektronische weg vastleggen van gegevens valt (logging), op grond van het voorgestelde artikel 32a.
Voorgesteld wordt de vastlegging van de verstrekking van politiegegevens op grond van paragraaf 3, thans in onderdeel f, te verplaatsen naar onderdeel b. De vastlegging omvat de doorgifte van politiegegevens, bedoeld in artikel 17, zesde lid, onderdeel b, en zevende lid, en de rechtstreekse doorgifte, bedoeld in artikel 17, achtste lid.
Toegevoegd zijn de onderdelen c en d. Dit betreft de redenen voor weigering van het recht op inzage en de feiten, gevolgen en genomen maatregelen rond datalekken (art. 15, derde lid, en 30, vijfde lid).

Tweede lid

Dit lid geeft een specifieke regeling voor de vastlegging van specifieke gegevens rond de doorgifte van politiegegevens aan een derde land of internationale organisatie, in de gevallen waarin de gegevens zijn vertrekt op basis van een beoordeling van de passende waarborgen van dat land of die organisatie door de verwerkingsverantwoordelijke of bij afwijkingen voor specifieke situaties (art. 37, derde lid en 38, derde lid, Rl). De vastlegging van deze gegevens dienst om de Autoriteit persoonsgegevens in staat te stellen de rechtmatigheid van de verstrekking te toetsen.

Vierde lid

De tekst van dit lid is aangepast vanwege de voorgestelde schrapping in het eerste lid van het huidige onderdeel d (geautomatiseerde vergelijking of het in combinatie met elkaar verwerken van politiegegevens, bedoeld in de artikelen 8, derde lid, en 11, eerste, tweede en vierde lid).

Artikel 32a. (logging)

1. De verwerkingsverantwoordelijke en de verwerker dragen zorg voor de vastlegging langs elektronische weg (logging) van ten minste de volgende verwerkingen van politiegegevens in geautomatiseerde systemen: het verzamelen, wijzigen, raadplegen, verstrekken onder meer in de vorm van doorgiften, combineren of vernietigen van politiegegevens.
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 politiegegevens en voor strafrechtelijke procedures.

Memorie van Toelichting - artikel 32a (logging) Wpg

Eerste lid

De logging betreft het geautomatiseerd vastleggen van gegevens over de verwerking van persoonsgegevens. De richtlijn bevat een verplichting voor de verwerkingsverantwoordelijke om logbestanden bij te houden van ten minste de volgende activiteiten in systemen voor geautomatiseerde verwerking: de verzameling, wijziging, raadpleging, verstrekking onder meer in de vorm van doorgiften, combinatie en het vernietigen van politiegegevens. In dit lid is deze verplichting vastgelegd. 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 (overweging 57 RI). Aldus maken de logbestanden van raadpleging en bekendmakingen 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. 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 loggingplicht omvat de schriftelijke vastlegging van bepaalde gegevens, op basis van de protocolplicht in het huidige artikel 32. Aldus vallen de in dit artikel vastgelegde verplichtingen tot vastlegging van de geautomatiseerde vergelijking of het in combinatie met elkaar verwerken van politiegegevens (eerste lid, onderdeel d), de hernieuwde verwerking van politiegegevens (eerste lid, onderdeel e), verwerkingen ten aanzien waarvan aanwijzingen bestaan dat zij onbevoegd of onrechtmatig zijn verricht (eerste lid, onderdeel g) en de geautomatiseerde vergelijking van gegevens (eerste lid, onderdeel h) onder de voorgestelde loggingplicht.

De logging betreft een geautomatiseerd proces, dat doorgaans standaard is ingebouwd in het informatiesysteem. Niettemin voorziet de richtlijn in een langere implementatietermijn voor de loggingplicht. Dit is in het algemeen deel van deze memorie aan de orde gekomen.

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).

Tweede lid

De vastgelegde gegevens kunnen uitsluitend worden gebruikt voor de controle van de rechtmatigheid van de gegevensverwerking, interne controles, ter waarborging van de integriteit en de beveiliging van de politiegegevens en voor strafrechtelijke procedures. Voor dit laatste kan worden gedacht aan strafvervolging op grond van ambtelijke corruptie, waarbij de gelogde gegevens kunnen worden gebruikt om aan te tonen dat een persoon op een bepaald tijdstip in het systeem gegevens heeft geraadpleegd, gewijzigd of gewist.