Staatsblad
van het Koninkrijk der Nederlanden

Jaargang 2018

115

Besluit van 18 april 2018, houdende regels inzake technische en organisatorische maatregelen met betrekking tot rechtstreeks geautomatiseerde toegang van de inlichtingen- en veiligheidsdiensten tot de gegevens verwerkt door informanten dan wel door ambtenaren van politie, van de Koninklijke marechaussee en van de rijksbelastingdienst (Besluit maatregelen rechtstreeks geautomatiseerde toegang inlichtingen- en veiligheidsdiensten)

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Op de voordracht van Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties van 15 augustus 2017, nr. 2017-0000212778, gedaan mede namens Onze Minister van Defensie;

Gelet op de artikelen 39, vierde lid, en 94, tweede lid, van de Wet op de inlichtingen- en veiligheidsdiensten 2017;

De Afdeling advisering van de Raad van State gehoord (advies van 25 oktober 2017, No. W04.17.0243/I);

Gezien het nader rapport van Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties van 17 april 2018, nr. 2017-000058532, uitgebracht mede namens Onze Minister van Defensie;

Hebben goedgevonden en verstaan:

Artikel 1

In dit besluit wordt verstaan onder:

a. *wet:* Wet op de inlichtingen- en veiligheidsdiensten 2017;

b. *toegangverlener:* de persoon of instantie die op grond van artikel 39, derde lid, onderscheidenlijk 94, tweede lid, rechtstreeks geautomatiseerde toegang verleent tot de gegevens, bedoeld in artikel 39, eerste lid, onderscheidenlijk 94, eerste lid, van de wet.

Artikel 2

1. De toegangverlener neemt de noodzakelijke technische en organisatorische maatregelen teneinde de vertrouwelijkheid van gegevensbevragingen door en gegevensverstrekkingen aan de diensten te waarborgen.

2. De maatregelen, bedoeld in het eerste lid, dienen in ieder geval te bestaan uit:

a. maatregelen gericht op de personen die kennis kunnen nemen van de gegevens die in het kader van rechtstreeks geautomatiseerde toegang door de diensten worden bevraagd en aan de diensten worden verstrekt;

b. maatregelen gericht op de toegang tot de ruimte waarin het informatiesysteem is geïnstalleerd, waarvoor de diensten rechtstreeks geautomatiseerde toegang wordt verleend;

c. maatregelen gericht op een deugdelijke werking en beveiliging van het informatiesysteem waarmee de rechtstreeks geautomatiseerde toegang wordt verleend, met inbegrip van de gegevens die zicht geven op de gegevensbevragingen door en gegevensverstrekkingen aan de diensten;

d. maatregelen gericht op het voorkomen, vaststellen en onderzoeken van een ongeoorloofde inbreuk op de vertrouwelijkheid van de gegevensbevragingen door en gegevensverstrekkingen aan de diensten.

3. Over de wijze waarop aan de voorgeschreven maatregelen uitvoering wordt gegeven vindt overleg plaats tussen de toegangverlener en de dienst.

Artikel 3

De toegangverlener stelt de desbetreffende dienst terstond op de hoogte, indien een ongeoorloofde inbreuk is gemaakt op de vertrouwelijkheid van de gegevensbevragingen door of gegevensverstrekkingen aan de diensten. Daarbij vermeldt de toegangverlener:

a. welke gegevens het betreft;

b. de wijze waarop de inbreuk heeft plaatsgevonden;

c. vanaf welke datum en welk tijdstip de inbreuk heeft plaatsgevonden;

d. welke maatregelen zijn genomen om verdere verspreiding van de gegevens tegen te gaan of herhaling van het gebeurde te voorkomen.

Artikel 4

1. Indien de toegangverlener de uitvoering van werkzaamheden uitbesteedt aan een derde en in dat kader de derde kennis neemt of kan nemen van gegevens betreffende gegevensbevragingen door en gegevensverstrekkingen aan de diensten, draagt de toegangverlener er zorg voor dat de derde zich verplicht:

a. de gegevens te beveiligen tegen kennisneming door onbevoegden;

b. met betrekking tot de gegevens geheimhouding te betrachten;

c. de ingevolge dit besluit gestelde maatregelen na te leven;

d. alle informatie te verstrekken die voor het toezicht op de naleving van de beveiligings- en geheimhoudingsverplichting noodzakelijk is.

2. De verplichtingen van de derde, bedoeld in het eerste lid, worden geregeld in een schriftelijke overeenkomst tussen de toegangverlener en de derde.

3. De dienst wordt tijdig op de hoogte gesteld van een voornemen van de toegangverlener tot het uitbesteden van de uitvoering van werkzaamheden aan een derde als bedoeld in het eerste lid. Op een daartoe strekkend verzoek van de dienst wordt inzage verleend in de overeenkomst, bedoeld in het tweede lid.

4. De toegangverlener is verantwoordelijk voor de naleving door de derde van de verplichtingen, bedoeld in het eerste lid.

Artikel 5

1. De diensten nemen de noodzakelijke technische en organisatorische maatregelen teneinde een rechtmatig gebruik door de diensten van de rechtstreeks geautomatiseerde toegang tot gegevens als bedoeld in de artikelen 39, derde lid, en 94, tweede lid, van de wet te waarborgen.

2. De maatregelen, bedoeld in het eerste lid, bestaan in ieder geval uit:

a. maatregelen gericht op de personen die het informatiesysteem van de toegangverlener waartoe de rechtstreeks geautomatiseerde toegang wordt verleend, kunnen bevragen en daaruit gegevens kunnen ontvangen;

b. maatregelen gericht op een deugdelijke werking van het systeem van de dienst waarmee rechtstreeks geautomatiseerde toegang wordt verkregen.

3. Het gebruik van het informatiesysteem van de dienst waarmee rechtstreeks geautomatiseerde toegang tot de gegevens wordt verkregen, wordt door de dienst vastgelegd. Daarbij wordt in ieder geval vastgelegd:

a. gegevens waarmee de medewerker die van het systeem gebruik heeft gemaakt kan worden geïdentificeerd;

b. de gegevens die in het kader van het gebruik van het systeem zijn ingevoerd;

c. de gegevens die met gebruikmaking van het systeem zijn ontvangen;

d. datum en tijdstip waarop van het systeem gebruik is gemaakt.

Artikel 6

Dit besluit treedt in werking op een bij koninklijk besluit te bepalen tijdstip.

Artikel 7

Dit besluit wordt aangehaald als: Besluit maatregelen rechtstreeks geautomatiseerde toegang inlichtingen- en veiligheidsdiensten.

Wassenaar, 18 april 2018

Willem-Alexander

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
K.H. Ollongren

De Minister van Defensie,
A.Th.B. Bijleveld-Schouten

Uitgegeven de *zesentwintigste* april 2018

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus

stb-2018-115
ISSN 0920 - 2064
's-Gravenhage 2018

NOTA VAN TOELICHTING

Algemeen

In artikel 39, eerste lid, van de wet is de algemene bevoegdheid van de diensten geregeld om zich bij de uitvoering van hun taak, dan wel ter ondersteuning van een goede taakuitvoering, voor het verzamelen van gegevens zich te wenden tot bestuursorganen, ambtenaren en voorts eenieder die geacht wordt de benodigde gegevens te kunnen verstrekken. Het gaat hier om het raadplegen van zogeheten informanten. De verstrekking van gegevens door informanten aan de dienst geschiedt op vrijwillige basis en kan verschillende vormen aannemen, zoals de verstrekking van documenten, het overdragen van digitale gegevensdragers met gegevens (geautomatiseerde gegevensbestanden), maar ook – zeker indien de informatieverstrekking een meer structureel karakter heeft – het verlenen van rechtstreeks geautomatiseerde toegang tot de bij een informant berustende gegevens. Onder dit laatste wordt een *on line*- en *real time* verbinding tussen de dienst en de verstrekkende persoon of instantie bedoeld, waarbij zonder menselijke tussenkomst aan de kant van de verstrekkende persoon of instantie, de desbetreffende dienst de gegevens die deze nodig heeft voor een goede taakuitvoering kan opvragen en verstrekt krijgt. In artikel 39, derde lid, van de wet zijn – om ter zake geen enkele onduidelijkheid te laten bestaan – de mogelijkheid tot verstrekking van geautomatiseerde gegevensbestanden en rechtstreeks geautomatiseerde toegang expliciet benoemd. In artikel 39, vierde lid, van de wet is bepaald dat bij of krachtens algemene maatregel van bestuur nadere regels worden gesteld met betrekking tot de te treffen technische en organisatorische maatregelen inzake rechtstreeks geautomatiseerde toegang. Onderhavig besluit voorziet daarin.

In artikel 94, eerste lid, van de wet is de verplichting van de ambtenaren van politie, de ambtenaren van de Koninklijke marechaussee en de ambtenaren van de rijksbelastingdienst neergelegd om desgevraagd dan wel uit eigen beweging onverwijld mededeling te doen van gegevens die voor een dienst van belang kunnen zijn. Het desgevraagd mededeling doen van gegevens die voor een dienst van belang kunnen zijn kan in bepaalde gevallen ook plaatsvinden door het verlenen van rechtstreeks geautomatiseerde toegang tot de door voormelde ambtenaren verwerkte gegevens. Behoudens de gevallen waarin deze mogelijkheid tot rechtstreeks geautomatiseerde toegang voor de diensten wettelijk is of wordt voorzien (vergelijk artikel 24 Wet politiegegevens), zal een dergelijke vorm van toegang op vrijwillige basis overeengekomen dienen te worden. Evenals bij artikel 39 is in artikel 94, tweede lid, van de wet bepaald, dat inzake de rechtstreeks geautomatiseerde toegang tot de gegevens bij of krachtens algemene maatregel van bestuur nadere regels worden gesteld met betrekking tot de te treffen technische en organisatorische maatregelen. Het gaat hierbij om vergelijkbare maatregelen als die welke op grond van artikel 39, vierde lid, dienen te worden gesteld. Het onderhavige besluit strekt dan ook mede ter uitvoering van artikel 94, tweede lid, van de wet.

De primaire focus van de maatregelen die in dit besluit zijn voorgeschreven richt zich op maatregelen aan de zijde van de persoon of instantie die rechtstreeks geautomatiseerde toegang verleent aan de diensten tot de door hem verwerkte gegevens (de toegangverlener), teneinde de vertrouwelijkheid van de bevragingen door de diensten te waarborgen. De reden daarvoor is de volgende. Vergelijking van door de diensten verwerkte gegevens met de gegevens die rechtstreeks geautomatiseerd door de verantwoordelijke voor de gegevensverwerking beschikbaar worden gesteld, vindt plaats om vast te stellen of er

verbanden bestaan tussen de desbetreffende gegevens. Het gaat hier om een verstrekking op hit/no hit basis; zodra er een hit is met gegevens bij de verantwoordelijke kunnen de gerelateerde gegevens aan de dienst worden verstrekt. In de praktijk kan het dan bijvoorbeeld gaan om de vergelijking van namen van targets met de naamgegevens die bijvoorbeeld bij een bestuursorgaan of een andere instantie berusten, waarbij bij een hit de bij het bestuursorgaan of de andere instantie berustende gegevens die aan die naam zijn gerelateerd aan de dienst kunnen worden verstrekt. De in het kader van de bevraging door de diensten ingevoerde gegevens in het systeem voor rechtstreeks geautomatiseerde toegang, alsmede de bij een hit aldus verstrekte gegevens, hebben naar hun aard een uiterst gevoelig – veelal staatsgeheim – karakter. Het kan hierbij gaan om namen van targets (onderzoekssubjecten) van de dienst, waarbij ingeval deze gegevens bij – niet daartoe gerechtigde – derden bekend zouden raken de nationale veiligheid ernstig in het geding kan komen. Maar het kan bijvoorbeeld ook gaan om de namen van (kandidaat)vertrouwensfunctionarissen waarnaar een veiligheidsonderzoek is ingesteld. Ook in dit geval gaat het om privacygevoelige en daarmee beschermingswaardige informatie. Het is dan ook noodzakelijk dat ter zake van de hier bedoelde gegevens bij de toegangverlener wordt voorzien in adequate beveiligingsmaatregelen teneinde een inbreuk op de vertrouwelijkheid van deze gegevens te voorkomen en, voor zover een dergelijke inbreuk wel heeft plaatsgevonden, te voorzien in maatregelen waarmee op een snelle en adequate wijze kan worden gereageerd. De artikelen 2 tot en met 4 van het besluit strekken daartoe. Het gaat daarbij om maatregelen, waarin te allen tijde dient te worden voorzien, waarbij de concrete invulling in overleg met de dienst plaatsvindt (zie artikel 2). Daarbij kan ook worden overeengekomen om nadere, aanvullende maatregelen te treffen. Waar het gaat om toepassing van artikel 39 van de wet, waarbij sprake is van gegevensverstrekking op vrijwillige basis, is de toegangverlener weliswaar verplicht om de maatregelen uit onderhavig besluit te treffen. Van een dwingend opleggen van een concrete invulling van de voorgeschreven maatregelen dan wel van aanvullende maatregelen door de diensten, kan echter geen sprake zijn. Indien de dienst van oordeel is dat de maatregelen die de toegangverlener wil treffen ontoereikend zijn, zal zij in overleg met de desbetreffende instantie kunnen bezien welke verbeteringen mogelijk zijn. Blijft een dienst van oordeel dat de voorgestelde maatregelen ontoereikend zijn, dan zal van de mogelijkheid van rechtstreeks geautomatiseerde toegang afgezien worden.

De in het besluit opgenomen maatregelen voor de toegangverlener laten overigens onverlet dat voor zover er bijzondere informatie in het geding is als bedoeld in het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013), ingevolge artikel 7, eerste lid, van dat besluit, waar het gaat om het buiten de rijksdienst brengen van bijzondere informatie (anders dan op grond van een wettelijke verplichting tot openbaarmaking), de eisen aan de beveiliging en het toezicht daarop uit dat besluit (ook) onverkort van kracht zijn.

Naast maatregelen aan de kant van de toegangverlener zal ook aan de kant van de diensten voorzien dienen te worden in de nodige maatregelen teneinde te verzekeren dat de bevraging slechts plaatsvindt door (of voor) degene die de desbetreffende informatie nodig heeft voor diens taakuitvoering en dat bevragingen (en de resultaten daarvan) worden vastgelegd (in verband met interne controle en het toezicht door de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD)). In onderhavig besluit zijn dan ook enkele bepalingen gesteld ter zake van de te treffen technische en organisatorische maatregelen aan de kant van de diensten (artikel 5). Deze zien met name op het gebruik dat gemaakt wordt van de mogelijkheid tot rechtstreeks geautomatiseerde toegang. Uit de

wet vloeien immers reeds de nodige plichten tot beveiliging van de gegevensverwerking door de diensten voort. Vergelijk de in de wet neergelegde zorgplichten voor de hoofden van de diensten (artikelen 23 en 24). Daar hoeft niet alsnog in te worden voorzien. De concrete invulling daarvan is bovendien uitgewerkt in gegevensbeschermingsbeleid dat elke dienst voor zijn eigen organisatie heeft opgesteld.

Tot slot wordt opgemerkt dat met het treffen van maatregelen als in dit besluit voorzien voor de toegangverlener kosten kunnen zijn gemoeid. Behoudens de gevallen waarin reeds voor de diensten een recht op rechtstreeks geautomatiseerde toegang is voorzien (artikel 24 Wet politiegegevens) is sprake van toegangverlening op vrijwillige basis, waaromtrent tussen de dienst en de toegangverlener overleg plaatsvindt. In dat overleg zal de kwestie inzake een eventuele kostenvergoeding aan de orde kunnen komen en kunnen ter zake afspraken worden gemaakt. De aard en omvang van een eventuele kostenvergoeding laten zich niet op voorhand vaststellen en zullen van geval tot geval verschillen. Bij de vaststelling van de kosten die voor vergoeding in aanmerking komen, zullen echter dezelfde uitgangspunten worden gehanteerd, zoals die in artikel 53, zevende lid, van de wet zijn verwoord. Dat betekent dat – voor zover van toepassing – naar redelijkheid de investerings-, exploitatie- en onderhoudskosten voor de te treffen voorziening alsmede de gemaakte administratie- en personeelskosten die rechtstreeks voortvloeien uit het verlenen van de rechtstreeks geautomatiseerde toegang voor vergoeding in aanmerking komen.

Artikelsgewijs

Artikel 2

In artikel 2, eerste lid, wordt in algemene zin aan de toegangverlener de zorgplicht opgelegd om de noodzakelijke technische en organisatorische maatregelen te treffen ter beveiliging van de vertrouwelijkheid van de gegevensbevragingen door en -verstrekkingen aan de diensten. In het tweede lid is dit – niet limitatief – uitgewerkt in een aantal maatregelen die de toegangverlener zonder meer dient te treffen. Daarbij is ruimte voor maatwerk, waarbij rekening kan worden gehouden met de specifieke omstandigheden van de toegangverlener (bijvoorbeeld aard en omvang van diens organisatie, de in gebruik zijnde informatiesystemen en de locatie). Voorts voorziet artikel 2, derde lid, erin dat over de wijze waarop aan de voorgeschreven maatregelen uitvoering wordt gegeven, overleg tussen de toegangverlener en de dienst plaatsvindt. Afspraken hierover kunnen door de dienst en de betreffende instantie in een overeenkomst (convenant) worden opgenomen.

De toegangverlener dient allereerst maatregelen te treffen gericht op de personen die kennis kunnen nemen van de gegevens die in het kader van rechtstreeks geautomatiseerde toegang ten behoeve van de diensten worden bevraagd en aan de diensten worden verstrekt (tweede lid, onder a). Daarbij moet worden gedacht aan het concreet aanwijzen van personeel dat – overeenkomstig hun functiebeschrijving – in het kader van de bevraging door c.q. verstrekking van gegevens aan de diensten en uit dien hoofde toegang hebben tot die gegevens of dat belast is met het beheer en het onderhoud van het desbetreffende informatiesysteem. Ook de ondertekening door het personeel van een geheimhoudingsverklaring is aan te merken als een dergelijke maatregel. Daarbij zij aangetekend dat op grond van artikel 135 van de wet reeds een geheimhoudingsplicht geldt voor eenieder die betrokken is bij de uitvoering van de wet.

Ten tweede dienen er maatregelen te worden getroffen die gericht zijn op de toegang tot de ruimte waarin het informatiesysteem is geïnstalleerd, waarvoor de diensten rechtstreeks geautomatiseerde toegang is verleend. Het gaat dan bijvoorbeeld om het treffen van deugdelijke fysieke beveiligingsmaatregelen die voorkomen dat ongeautoriseerde personen toegang krijgen tot de ruimte waar het desbetreffende informatiesysteem is geplaatst en dat pogingen tot ongeautoriseerde toegang tijdig worden onderkend en dat daarop wordt geïntervenieerd. Een mogelijkheid kan zijn om in verband met de rechtstreeks geautomatiseerde toegang van de diensten tot de gegevens te voorzien in een afzonderlijk systeem (duplicaat) en dat in een afgeschermde ruimte te plaatsen.

Ten derde dienen er maatregelen te worden getroffen gericht op een deugdelijke werking en beveiliging van het informatiesysteem waarmee de rechtstreeks geautomatiseerde toegang wordt verleend, met inbegrip van de gegevens die zicht geven op de gegevensbevragingen door en -verstrekkingen aan de diensten. Daarnaast moet er – ten vierde – voorzien zijn in maatregelen gericht op het voorkomen, vaststellen en onderzoeken van een ongeoorloofde inbreuk op de vertrouwelijkheid van de gegevensbevragingen door en -verstrekkingen aan de diensten. Anders dan de onder a en b genoemde maatregelen, betreft het hier maatregelen die (de toegang tot) het informatiesysteem zelf betreffen. Daarbij kan men denken aan het inbouwen van een systeem van persoonsgebonden authenticatie, waardoor uitsluitend die personen toegang kunnen krijgen die daartoe zijn geautoriseerd. Zo zal er ook voorzien moeten worden in een logging van wie toegang tot het informatiesysteem heeft verkregen en de handelingen die in dat kader zijn verricht. Daarnaast dient er voorzien te worden in maatregelen die pogingen om ongeautoriseerde toegang te verkrijgen tot het informatiesysteem tijdig detecteren en het mogelijk maken om daarop te interveniëren. De beveiliging dient van dien aard te zijn dat gedegen onderzoek naar (vermoede) inbreuken mogelijk is. De twee laatstgenoemde maatregelen hangen samen met de in artikel 3 neergelegde plicht voor de toegangverlener om de dienst terstond op de hoogte te stellen, indien op de vertrouwelijkheid van de gegevensbevragingen door en gegevensverstrekkingen aan de dienst inbreuk is gemaakt (compromittering). Voorts moet gedacht worden aan beveiligingsmaatregelen die getroffen dienen te worden in geval van onderhoud en reparatie van het informatiesysteem.

Artikel 3

Gelet op de aard van de gegevens is het van het grootste belang dat niet daartoe gerechtigde personen daarvan geen kennis kunnen nemen. Het gaat immers om gegevens, vaak met een staatsgeheim karakter, waarvan de compromittering ernstige gevolgen kan hebben voor de onderzoeken die door de dienst worden verricht en waarmee uiteindelijk de nationale veiligheid kan worden geschaad. In verband hiermee dienen niet alleen in het informatiesysteem van de toegangverlener maatregelen te worden ingebouwd die ongeoorloofde toegang tegengaan, maar ook (pogingen tot) ongeoorloofde toegang detecteren (zie artikel 2). In het verlengde daarvan dient ook te worden voorzien in maatregelen ingeval door een toegangverlener wordt vastgesteld dat een ongeoorloofde inbreuk heeft plaatsgevonden. In artikel 3 van het besluit is dan ook de verplichting voor de toegangverlener opgenomen om de dienst terstond op de hoogte te stellen, indien op de vertrouwelijkheid van de gegevensbevraging door en gegevensverstrekking aan de dienst een ongeoorloofde inbreuk is gemaakt. Daarbij dient hij aan te geven welke gegevens het betreft. Voorts dient te worden vermeld op welke wijze de inbreuk heeft plaatsgevonden en vanaf welke datum en welk tijdstip. Dit laatste gegeven is met name van belang voor de dienst om de omvang van de

mogelijke schade in te kunnen schatten. Tot slot dient te worden aangegeven welke maatregelen door de toegangverlener zijn genomen om verdere verspreiding van de gegevens tegen te gaan of herhaling van het gebeurde te voorkomen. Op basis van deze gegevens zal de dienst de maatregelen kunnen nemen die deze aangewezen acht om de gevolgen voor de onderzoeken van de dienst – en daarmee ook de schade voor de nationale veiligheid – tot een minimum te beperken. Ingeval de inbreuk staatsgeheime informatie betreft, zal bovendien overeenkomstig het bepaalde in het VIRBI 2013 een onderzoek dienen plaats te vinden. Tot slot wordt opgemerkt, dat indien het vermoeden rijst dat er een strafbaar feit is gepleegd (artikel 98 e.v. alsmede 272 Wetboek van Strafrecht) daarvan aangifte zal worden gedaan, hetgeen kan resulteren in een strafrechtelijk onderzoek.

Artikel 4

In de praktijk kan het voorkomen dat een toegangverlener de uitvoering aan werkzaamheden uitbesteedt aan een derde en dat die derde in dat kader kennisneemt of kan nemen van gegevens betreffende de gegevensbevragingen en -verstrekkingen aan de diensten. Voor zover hiervan reeds sprake is op het moment dat tussen de dienst en de toegangverlener overleg plaatsvindt over de mogelijkheid van rechtstreeks geautomatiseerde toegang, zal dit feit onderdeel van dat overleg uitmaken en door de dienst worden betrokken bij het antwoord op de vraag of van de geboden mogelijkheid van rechtstreekse toegang gebruik moet worden gemaakt. Daarnaast kan zich de situatie voordoen dat indien er door de dienst reeds gebruik wordt gemaakt van de mogelijkheid van rechtsreeks geautomatiseerde toegang, de toegangverlener de uitvoering van werkzaamheden als hier bedoeld alsnog wenst uit te besteden. In dat geval is de toegangverlener verplicht om de dienst tijdig van een voornemen daartoe op de hoogte te stellen (derde lid). De dienst kan aldus bezien of voortgezet gebruik van de mogelijkheid tot rechtstreeks geautomatiseerde toegang verantwoord is of dat deze dient te worden beëindigd.

In beide gevallen, zowel waar het gaat om een bestaande als een voorgenomen uitbesteding, dient de toegangverlener er zorg voor te dragen dat de derde waaraan de werkzaamheden zijn of worden uitbesteed zich in een schriftelijke overeenkomst verplicht (a) de gegevens te beveiligen tegen kennisneming door onbevoegden, (b) met betrekking tot de gegevens geheimhouding te betrachten, (c) de ingevolge dit besluit gestelde maatregelen na te leven en (d) alle informatie te verstrekken die voor het toezicht op de naleving van de beveiligings- en geheimhoudingsverplichting noodzakelijk is. De dienst wordt desgevraagd inzage verleend in deze overeenkomst. De toegangverlener is verantwoordelijk voor de naleving van de verplichtingen door de derde.

Artikel 5

In artikel 5 worden enkele technische en organisatorische maatregelen voorgeschreven, die de diensten kunnen en dienen te treffen in het geval dat zij rechtstreeks geautomatiseerde toegang tot gegevens bij een bepaalde instantie hebben verkregen op grond van artikel 39, derde lid, dan wel artikel 94, tweede lid, van de wet. Allereerst wordt bepaald dat maatregelen dienen te worden getroffen die gericht zijn op de personen die het informatiesysteem van de toegangverlener waartoe rechtstreeks geautomatiseerde toegang wordt verleend kunnen bevragen en daaruit gegevens kunnen ontvangen. Hierbij kan worden gedacht aan een maatregel die het raadplegen van het informatiesysteem van de toegangverlener beperkt tot die medewerkers van de dienst die, bij uitsluiting van anderen, daartoe zijn geautoriseerd. Deze medewerkers verstrekken de

gevraagde gegevens vervolgens aan de medewerker van de dienst die daarom verzocht heeft. Daarnaast moeten de diensten maatregelen treffen gericht op een deugdelijke werking van het eigen informatiesysteem waarmee de rechtstreeks geautomatiseerde toegang tot de gegevens bij de toegangverlener wordt verkregen. Zo kan ervoor gekozen worden het informatiesysteem geen geïntegreerd onderdeel uit te doen maken van de door de desbetreffende dienst in het kader van de reguliere bedrijfsvoering gebruikte informatiesystemen. Veelal zal voor de rechtstreeks geautomatiseerde toegang gebruik gemaakt worden van een stand alone-systeem. Dit biedt – mede door aanvullende maatregelen, zoals plaatsing in een afzonderlijke (beveiligde) ruimte – deugdelijke mogelijkheden en waarborgen voor rechtmatig gebruik van de rechtstreeks geautomatiseerde toegang. Het is echter denkbaar dat naar aanleiding van technologische ontwikkelingen in de (nabije) toekomst een andersoortig systeem of andere werkwijze wordt gehanteerd wanneer dit gelijke of zelfs betere waarborgen biedt. Tot slot dient van het gebruik verslaglegging (logging) plaats te vinden, waarbij in ieder geval worden vastgelegd waarmee de medewerker die van het systeem gebruik heeft gemaakt kan worden geïdentificeerd (bijvoorbeeld een personeelsnummer of personeelskenmerk), welke gegevens in het systeem zijn ingevoerd in het kader van de bevraging, de gegevens die in reactie op de bevraging zijn ontvangen alsmede datum en tijdstip waarop van het systeem gebruik is gemaakt. Deze gegevens zijn van belang voor het interne toezicht op het gebruik van het systeem, maar bijvoorbeeld ook voor het toezicht door de CTIVD die aldus kan toetsen of er op een rechtmatige wijze gebruik van is gemaakt. Op de aldus vastgelegde gegevens zijn de algemene bepalingen uit paragraaf 3.1 van de wet van toepassing. Dat betekent dat zodra deze gegevens, gelet op het doel waarvoor zij worden verwerkt, hun betekenis hebben verloren, ze dienen te worden verwijderd (artikel 20, eerste lid). Ingevolge artikel 20, derde lid, worden de verwijderde gegevens vernietigd, tenzij wettelijke regels omtrent bewaring daaraan in de weg staan; dit laatste betekent dat acht dient te worden geslagen op hetgeen in de selectielijst op grond van de Archiefwet 1995 ter zake is bepaald (zie ook artikel 21 van de wet).

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
K.H. Ollongren