Privacy Impact Assessment (PIA)

Wetsvoorstel gegevensverwerking en meldplicht cybersecurity

1. Noodzaak Wet gegevensverwerking en meldplicht cybersecurity

   Een wettelijke meldplicht voor ICT-inbreuken is aangekondigd in een brief aan de Tweede Kamer van 6 juli 2012, naar aanleiding van een verzoek van de Kamer om te komen tot de wettelijke vastlegging van een 'security breach notification' bij het Nationaal Cyber Security Centrum (NCSC) voor organisaties die betrokken zijn bij voor de samenleving vitale informatiesystemen. Aanleiding voor dat verzoek waren de gebeurtenissen bij het bedrijf DigiNotar in het najaar van 2011. Deze ICT-inbreuk heeft het toegenomen belang en de onderlinge verwevenheid van ICT-systemen bij de overheid en (overige) vitale sectoren nadrukkelijk zichtbaar gemaakt. De meldplicht sluit aan bij de meldplicht zoals voorgeschreven in de komende EU-richtlijn over netwerk- en informatiebeveiliging.

   Naar aanleiding van het Pobelka-incident in 2013 heeft de Minister van Veiligheid en Justitie (VenJ) onderzocht of er voldoende rechtsbasis is voor de verwerking van gegevens bij de uitvoering, door het NCSC, van zijn taken op het terrein van cybersecurity. In zijn brief van 12 december 2013 heeft de Minister de Tweede Kamer bericht dat het wenselijk is om die taken en die verwerking van een steviger wettelijke grondslag te voorzien, onder meer met het oog op het verwerken van persoonsgegevens.

2. Doel van het PIA

   Bij de uitvoering van de taken op het terrein van cybersecurity die het NCSC namens de Staatssecretaris van VenJ vervult, verwerkt het NCSC persoonsgegevens. Deze verwerking, die net als de taken in het kader waarvan deze geschiedt in het wetsvoorstel worden geregeld, wordt getoetst om eventuele privacyrisico's te voorkomen of beperken. Een PIA is daarbij een hulpmiddel om bij ontwikkeling van beleid of wetgeving of bouw van ICT-systemen en aanleg van databestanden, privacyrisico's op gestructureerde en heldere wijze in kaart te brengen.

   Een PIA is verplicht (sinds september 2013) bij ICT-projecten. De opdrachtgever van een project waarvoor een PIA wordt gedaan, gebruikt de uitkomsten van het PIA om een project goed in te richten op basis van de privacyrisico's. Daarnaast biedt het PIA een mogelijkheid voor het NCSC om op transparante wijze de verwerking van persoonsgegevens binnen het NCSC inzichtelijk te maken.

3. Doorlooptijd PIA

   Dit PIA is op 3 september 2014 opgesteld en laatstelijk geactualiseerd in juni 2016.

I. Basisinformatie: type persoonsgegevens, type verwerking en noodzaak/gegevensminimalisering

1. Wilt u als verantwoordelijke persoonsgegevens gaan gebruiken voor de verwerking die u voorziet? Zo ja, van welk type?

De verantwoordelijke voor de verwerking van persoonsgegevens op grond van de Wet gegevensverwerking en meldplicht cybersecurity is de Minister van VenJ, maar ingevolge de huidige portefeuilleverdeling de Staatssecretaris van VenJ.

Op grond van dit wetsvoorstel kan de Staatssecretaris van VenJ persoonsgegevens verwerken die noodzakelijk zijn voor het uitvoeren van taken ter voorkoming of beperking van het uitvallen van de beschikbaarheid of het verlies van integriteit van informatiesystemen van vitale aanbieders en andere aanbieders die deel uitmaken van de rijksoverheid en ter verdere versterking van de digitale weerbaarheid van de Nederlandse samenleving. Ten behoeve van deze taken zal het - hoewel niet uitputtend - in ieder geval gaan om:

- bij het incident betrokken IP-adressen, e-mailadressen of domeinnamen, voor zover deze als persoonsgegevens kunnen worden aangemerkt;
- contactgegevens van bijvoorbeeld de melder (naam, e-mailadres, telefoonnummer);
- gebruikersnamen, wachtwoorden en andere inloggegevens; zie vraag I.2c.

Afhankelijk van de aard van het incident en de reactie daarop is het niet op voorhand uit te sluiten dat het NCSC ook andere gegevens in het kader van de melding ontvangt, waaronder gegevens die niet strikt noodzakelijk zijn voor het uitvoeren van de taken van het NCSC. Deze laatste categorie gegevens wordt zo snel mogelijk vernietigd.

2. Andere specifieke persoonsgegevens?

2a. Is het de bedoeling om gegevens over de financiële of economische situatie van betrokkenen, of andere gegevens die kunnen leiden tot stigmatisering of uitsluiting de verwerken?

Nee

2b. Is het de bedoeling om gegevens over kwetsbare groepen of personen te verwerken?

Over het algemeen verwerkt het NCSC geen gegevens van kwetsbare groepen of personen. In het kader van 'responsible disclosure', waarbij personen informatie omtrent gevonden kwetsbaarheden in vertrouwen met het NCSC delen, kan het NCSC contactgegevens van deze personen verwerken. Deze personen kunnen in feite worden aangemerkt als een kwetsbare groep personen.

2c. Is het de bedoeling gebruikersnamen, wachtwoorden en andere inloggegevens te verwerken?

Afhankelijk van de informatie die het NCSC aangaande een incident of kwetsbaarheid ontvangt, en/of de eventuele vervolgstappen die het NCSC op basis daarvan onderneemt, bijvoorbeeld in het kader van de technische ondersteuning die het NCSC aan getroffen organisaties biedt, kunnen gebruikersnamen, wachtwoorden en andere inloggegevens van bijvoorbeeld medewerkers van getroffen vitale- en rijksoverheidsorganisaties worden verwerkt.

2d. Is het de bedoeling om uniek identificerende gegevens, zoals biometrische gegevens, te verwerken?

Nee

2e. Is het de bedoeling om het BSN nummer, of een ander persoonsgebonden nummer te verwerken?

Nee

3. Kan van elk van de onder vraag I.1 en vraag I.2 opgevoerde typen persoonsgegevens worden gesteld dat zij beleidsmatig of technisch direct van belang en onontbeerlijk zijn het bereiken van de beleidsdoelstelling? Wat zou er precies niet inzichtelijk worden als ervoor wordt gekozen bepaalde gegevens niet te verwerken? Licht per te verwerken persoonsgegevens toe.

Ja, de verwerking beperkt zich tot die persoonsgegevens die technisch of beleidsmatig noodzakelijk zijn voor de uitoefening van de onder vraag I.5 benoemde taken ter voorkoming van of beperking van de uitval van de beschikbaarheid en het verlies van integriteit van informatiesystemen van vitale- en rijksoverheidsorganisaties en de verdere versterking van de digitale weerbaarheid van de Nederlandse samenleving. Zo zijn contactgegevens noodzakelijk om gevolg te geven aan een melding, bijvoorbeeld voor het verlenen van hulp of het geven van advies. Het verwerken van bij een incident betrokken IP-adressen, e-mailadressen of domeinnamen is noodzakelijk om onderzoek te doen naar de aard en omvang van het incident, voor het bepalen van het risico op andere gelijksoortige incidenten of voor het nemen van vervolgacties ter voorkoming of beperking van ernstige maatschappelijke gevolgen. Zonder deze gegevens kan het NCSC bovenbedoelde taken niet vervullen.

Afhankelijk van de aard van het incident en de eventuele navolging hierop is het niet op voorhand uit te sluiten dat het NCSC ook andere gegevens in het kader van de melding ontvangt, die niet strikt noodzakelijk zijn voor het uitvoeren van de taken. Zie voor het regime met betrekking tot dergelijke gegevens vraag 7.

4. Kan als het gaat om gevoelige persoonsgegevens hetzelfde beleidseffect of technisch resultaat worden bereikt op een van de volgende wijzen: (a) door (gecombineerd) gebruik van normale persoonsgegevens, (b) door gebruik van geanonimiseerde of gepseudonimiseerde gegevens?

Nee

5. In welk breder wettelijk, beleidsmatig of technisch kader wordt het voorziene beleid/databestand/informatiesysteem ontwikkeld en wat voor soort(en) verwerking(en) van persoonsgegevens gaan hiervan deel uitmaken bij het voorziene traject? Wordt hierbij gebruik gemaakt van (nieuwe) technologie of informatiesystemen?

Dit wetsvoorstel verstevigt het wettelijk kader voor gegevensverwerking door het NCSC in het kader van de uitoefening van zijn taken ter voorkoming of beperking van de uitval van de beschikbaarheid of het verlies van integriteit van informatiesystemen van vitale- en rijksoverheidsorganisaties en verdere versterking van de digitale weerbaarheid van de Nederlandse samenleving. Daarbij gaat het om de volgende taken:

a. het bijstaan van vitale aanbieders en andere aanbieders die deel uitmaken van de rijksoverheid bij het treffen van maatregelen om de beschikbaarheid en betrouwbaarheid van producten of diensten te waarborgen of te herstellen;
b. het informeren en adviseren van genoemde aanbieders en anderen in en buiten Nederland over dreigingen en incidenten met betrekking tot informatiesystemen van deze aanbieders;
c. het verrichten van analyses en technisch onderzoek ten behoeve van de onder a en b genoemde taken, naar aanleiding van dreigingen en incidenten (of aanwijzingen daarvoor) met betrekking tot genoemde informatiesystemen, niet zijnde onderzoek naar personen of organisaties die voor die dreigingen en incidenten verantwoordelijk zijn of daaraan bijdragen.

Voorts heeft het NCSC, ter voorkoming van nadelige maatschappelijke gevolgen, tot taak: het verstrekken van door bovenvermelde analyses en technisch onderzoek verkregen gegevens over dreigingen en incidenten met betrekking tot andere dan bovengenoemde informatiesystemen aan:

- organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek daarover te informeren;
- computercrisisteams, aangewezen bij regeling van de Staatssecretaris van VenJ of behorend tot een bij die regeling aangewezen categorie;
- aanbieders van internettoegangs- en internetcommunicatiediensten ten behoeve van het informeren van gebruikers van die diensten.

Bij het uitvoeren van bovenstaande taken worden alleen persoonsgegevens verwerkt die noodzakelijk zijn voor de uitvoering van deze taken. Het gaat hierbij om het ontvangen, opslaan en correleren van persoonsgegevens. Deze gegevens kunnen met het oog op de doeleinden voor de verwerking – indien en voor zover noodzakelijk voor het verwezenlijken van deze doeleinden – worden gedeeld met bijvoorbeeld vitale aanbieders of andere aanbieders die deel uitmaken van de rijksoverheid. Voor het verwerken van de persoonsgegevens wordt gebruik gemaakt van technologieën en informatiesystemen.

II. Doelbinding, koppeling, kwaliteit en profilering

1. Hebt u het/de specifieke doel(en) waarvoor u de persoonsgegevens gaat verwerken in detail vastgesteld? Geld hiervoor één en hetzelfde specifieke doel?

Ja. Het doel van gegevensverwerking op basis van het wetsvoorstel is het voorkomen of beperken van het uitvallen van de beschikbaarheid of het verlies van integriteit van voor de samenleving vitale producten en diensten en de verdere versterking van de digitale weerbaarheid van de Nederlandse samenleving (artikel 2, eerste lid) en het voorkomen van negatieve maatschappelijke gevolgen als gevolg van ICT-incidenten (artikel 2, tweede lid).

2. Gaat het bij het project/systeem om gebruik van nieuwe persoonsgegevens voor een bestaand doel, of bestaande doelen binnen al bestaande systemen?

Nee. Er is geen sprake van de verwerking van nieuwe persoonsgegevens voor bestaande doeleinden ten opzichte van de huidige situatie.

3. Gaat het bij het project/systeem om het nastreven van nieuwe/aanvullende doeleinden door bestaande persoonsgegevens, of verzamelingen daarvan, te gebruiken, vergelijken, delen, koppelen of anderszins verder te verwerken? (scenario toevoeging doeleinden). Zo ja, hebben alle personen/instanties/systemen die betrokken zijn bij de verwerking dezelfde doelstelling met de verwerking van de desbetreffende persoonsgegevens of is daarmee spanning mogelijk gelet op hun taak of hun belang? Gelden dezelfde doelen voor het hele proces?

Het verwerken van persoonsgegevens in het kader van de uitoefening van de eerste drie hierboven genoemde taken (bijstand, informeren en adviseren, analyses en technisch onderzoek) geschiedt thans al door het NCSC ten behoeve van het voorkomen of beperken van de uitval van de beschikbaarheid of het verlies van de integriteit van voor de samenleving vitale producten en diensten en het verder versterken van de digitale weerbaarheid van de Nederlandse samenleving. Hoewel hiervoor een voldoende wettelijke grondslag kan worden vastgesteld, wordt de grondslag voor deze verwerking met dit wetsvoorstel verder verstevigd. Ten aanzien hiervan is geen sprake van verwerking van persoonsgegevens voor nieuwe doeleinden.

Persoonsgegevens betreffende incidenten aangaande andere informatiesystemen dan die van de rijksoverheids- of vitale organisaties, die worden verkregen bij de analyses ten behoeve van de hulpverlening aan rijksoverheids- en vitale organisaties, worden thans na een eerste verwerking direct vernietigd. Op grond van dit wetsvoorstel kunnen deze persoonsgegevens voortaan worden

verstrekt aan andere, in het wetsvoorstel genoemde partijen, ter voorkoming van nadelige maatschappelijke gevolgen. Dit betreft een verwerking van reeds bestaande gegevens voor een nieuw doeleinde.

4. Indien u positief hebt geantwoord op vragen II.2 of II.3, hoe wordt een dergelijk voorgenomen gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) gemeld aan: (a) de functionaris voor de gegevensbescherming, of (b) de Autoriteit persoonsgegevens indien er geen FG is?

De verwerking van persoonsgegevens voor nieuwe doeleinden zal, in aanvulling op de huidige melding, worden gemeld bij de functionaris voor de gegevensbescherming van het Ministerie van VenJ.

5. Indien u positief geantwoord hebt op vragen II.2 of II.3, welke (nadere) controles op een dergelijk gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) zijn voorzien?

Hiervoor wordt aansluiting gezocht bij reeds bestaande processen en procedures voor controles op gebruik van persoonsgegevens.

6. Welke periodieke en incidentele controles zijn voorzien om de juistheid, nauwkeurigheid en actualiteit van de in het beleidsvoorstel, wetsvoorstel of overheids-ICT-systeem verwerkte persoonsgegevens na te gaan?

Beleid voor het controleren van de juistheid, nauwkeurigheid en actualiteit van de verwerkte persoonsgegevens is in voorbereiding. Afronding is voorzien vóór 1 januari 2017.

7. Zullen de verzamelde/verwerkte persoonsgegevens gebruikt worden om het gedrag, de aanwezigheid of de prestaties van mensen in kaart te brengen en/of te beoordelen en/of te voorspellen? Zijn de betrokkenen daarvan op de hoogte? Zijn de gegevens die hiervoor worden gebruikt, afkomstig uit verschillende (eventueel externe) bronnen en zijn zij oorspronkelijk voor andere doelen verzameld?

Nee

8. Wordt bij deze analyse/beoordeling/voorspelling gebruik gemaakt van vergelijking van persoonsgegevens die technisch geautomatiseerd is (d.w.z. niet door mensen zelf wordt uitgevoerd)? Zo ja, hoe wordt geregeld dat, indien dit geautomatiseerde proces tot een beoordeling of voorspelling over een bepaalde persoon leidt, hierop pas concrete actie wordt ondernomen na tussenkomst en (tweede) controle van (menselijk) personeel?

Nee, idem II.7.

III. Betrokken instanties/systemen en verantwoordelijkheid

1. Welke interne en externe instantie(s) en/of systemen is/zijn betrokken bij de voorziene verwerking in elk van de onder I.5 onderscheiden fasen? Welke verstrekkers zijn er en welke ontvangers? Welke bestanden of deelbestanden en welke infrastructuren?

Om de veiligheid en integriteit van informatiesystemen van vitale aanbieders en (andere) rijksoverheidsorganisaties te waarborgen, en de digitale weerbaarheid van de samenleving verder te versterken, moeten gegevens, waaronder persoonsgegevens, worden verwerkt. Deze verwerking geschiedt primair bij het NCSC. Wanneer het ten behoeve van de in artikel 2 genoemde doeleinden en taken noodzakelijk is, kunnen binnen de overige kaders van het

wetsvoorstel en met inachtneming van de Wet bescherming persoonsgegevens (Wbp) gegevens worden gedeeld met andere organisaties, meer in het bijzonder:

- vitale aanbieders en andere aanbieders die deel uitmaken van de rijksoverheid;
- door de Staatssecretaris van VenJ bij regeling aangewezen computercrisisteams (Computer Emergency Respons Teams, CERT's), in of buiten Nederland;
- de Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst;
- andere, voor een vitale sector verantwoordelijke, ministeries;
- organisaties die tot taak hebben om andere organisaties of het publiek over ICT-dreigingen en -incidenten te informeren, aanbieders van internettoegangs- en internetcommunicatiediensten;
- andere organisaties (bijv. OM) en het publiek.

2. Is (in ieder stadium) duidelijk wie verantwoordelijk is voor de verwerking van de persoonsgegevens? Zo ja, is deze persoon of organisatie daarop voldoende voorbereid en geëquipeerd wat betreft de nodige voorzieningen en maatregelen, waaronder middelen, beleid, taakverdeling, procedures en intern toezicht?

Voor de verwerking van persoonsgegevens door het NCSC is de Staatssecretaris van VenJ verantwoordelijk. De staatssecretaris is in voldoende mate voorbereid op deze verwerkingen door getroffen voorzieningen en (ontwikkeling van) beleid, behoudens de beantwoording van vraag 6 en 7.

3. Wie binnen uw organisatie, en elk van de andere betrokken organisaties, krijgen precies toegang tot de persoonsgegevens? Bestaat de kans dat bij het gebruik ervan de gegevens ter beschikking komen van onbevoegden?

Slechts medewerkers van het NCSC die met de uitvoering van de eerder genoemde taken zijn belast hebben toegang tot de voor die taken verwerkte persoonsgegevens. De kans op gebruik van de gegevens door onbevoegden is gering. Alle maatregelen passen in het regime dat bij het NCSC reeds van toepassing is met betrekking tot strikte beveiligingsmaatregelen op basis waarvan onbevoegden geen toegang wordt gegeven tot gegevens die bij het NCSC worden verwerkt.

4. Geldt voor een of meer van de betrokken instanties een beperking van de mogelijkheid om persoonsgegevens te verwerken als gevolg van geheimhoudingsverplichtingen (in verband met functie/wet)?

Niet van toepassing.

5. Zijn alle stappen van de verwerking in de zin van soorten gegevens en uitwisselingen, in kaart gebracht of te brengen, zodanig dat daardoor voor de betrokkenen inzichtelijk is bij wie, waarom en hoe de persoonsgegevens worden verwerkt?

Ja, de stappen van verwerking zijn op verzoek van de betrokkene in kaart te brengen.

6. Zijn er beleid en procedures voorzien voor het creëren en bijhouden van een verzameling van de persoonsgegevens die u wilt gaan gebruiken? Zo ja, hoe vaak en door wie zal de verwerking worden gecontroleerd? Omvat de verzameling een verwerking die namens u wordt uitgevoerd (bijvoorbeeld door een onderaannemer)?

Ja, voorafgaand aan het aanleggen van (nieuwe) specifieke verzamelingen van persoonsgegevens wordt een vaste procedure van 'checks and balances' gevolgd. Zo wordt standaard een juridische toets gedaan op deze voorgenomen verwerkingen aan de hand van de vereisten van de Wbp. Deze toets maakt deel uit van de besluitvorming betreffende het aanleggen en bijhouden van die verzameling. Controle op het creëren en bijhouden van verzamelingen persoonsgegevens vindt

daarmee voorafgaand aan iedere nieuwe verwerking plaats. De functionaris voor de gegevensbescherming van het Ministerie van VenJ houdt hier toezicht op. Van verwerkingen door bijvoorbeeld een onderaannemer is geen sprake.

7. Is er sprake van overdracht van persoonsgegevens naar een (overheids)instantie buiten de EU/EER? Heeft dit land een niveau van gegevensbescherming dat als passend is beoordeeld door een besluit van de Europese Commissie of de Minister van VenJ? Worden daarbij alle of een gedeelte van de persoonsgegevens doorgegeven?

Hiervan kan sprake zijn als gegevens worden gedeeld met een buitenlands CERT dat zich niet in de EU/EER-zone bevindt. Met welke CERT's persoonsgegevens kunnen worden gedeeld, wordt door de Staatssecretaris van VenJ bij regeling bepaald. Ten behoeve daarvan wordt onder meer beoordeeld of ten aanzien van een CERT sprake is van een passend niveau van gegevensbescherming.

Gegevens worden alleen met dat CERT gedeeld indien en voor zover dat noodzakelijk is ten behoeve van de in artikel 2 genoemde doeleinden en taken en ook overigens wettelijk is toegestaan.

IV. Beveiliging en bewaring/vernietiging

1. Is het beleid met betrekking tot gegevensbeveiliging binnen uw organisatie op orde? Zo ja, wie/welke afdeling(en) is/zijn binnen de organisatie verantwoordelijk voor het opstellen, implementeren en handhaven hiervan? Is dit beleid specifiek gericht op gegevensbescherming en gegevensbeveiliging?

Ja. In de Baseline Informatiebeveiliging Rijksdienst (BIR) is de visie op informatiebeveiliging voor de rijksoverheid opgenomen. Hierin staat dat gegevensbeveiliging centraal staat bij beleid. In de Baseline staat tevens dat automatische controle plaatsvindt op virussen, trojans en andere malware. Binnen het Ministerie van VenJ is de Beveiligingsautoriteit (BVA-VenJ) belast met het opstellen van een ministerie-breed beveiligingsbeleid op basis van de BIR. Dit beleid wordt ten behoeve van de NCTV (waar het NCSC deel van uitmaakt) nader uitgewerkt en waar nodig voorzien van NCTV-specifieke bepalingen door de Beveiligingscoördinator van de NCTV (BVC-NCTV). De afdelingshoofden binnen het NCSC zijn primair verantwoordelijk voor de uitvoering van dit beveiligingsbeleid. Daarnaast ziet de functionaris voor de gegevensbescherming van het Ministerie van VenJ specifiek toe op de bescherming van persoonsgegevens die binnen VenJ worden verwerkt.

2. Indien (een deel van) de verwerking bij een bewerker plaatsvindt, hoe draagt u zorg voor de gegevensbeveiliging, en het toezicht daarop, bij die bewerker?

Niet van toepassing.

3. Welke technische en organisatorische beveiligingsmaatregelen zijn getroffen ter voorkoming van niet-geautoriseerde of onrechtmatige verwerking/misbruik van (a) gegevens die in een geautomatiseerd format staan (bijv. wachtwoord-bescherming, versleuteling, encryptie) en (b) gegevens die handmatig zijn opgetekend bijv. sloten op kasten)? Is er een hoger beschermingsniveau om gevoelige persoonsgegevens te beveiligen?

De gegevens staan opgeslagen op een server bij het NCSC in Den Haag. Bij het NCSC zijn als onderdeel van de Rijksdienst beveiligingsmaatregelen op grond van het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIR-BI 2013) en de BIR geïmplementeerd.

Hierbij kan worden gedacht aan de volgende maatregelen:

- Versleutelde opslag van incidentinformatie
- Fysieke en digitale toegangscontrole
- Role-based toegang tot informatie ('need to know')
- Beveiligde digitale omgevingen
- Opslag van fysieke data en datadragers in kluizen
- Screenings van medewerkers
- Rubriceringsvoorschriften voor vertrouwelijke documenten
- Beperkte toegang
- Beveiligd vervoer

4. Welke procedures bestaan er in geval van inbreuken op beveiligingsvoorschriften, en voor het detecteren ervan? Is er een calamiteitenplan om het gevolg van een onvoorziene gebeurtenis waarbij persoonsgegevens worden blootgesteld aan onrechtmatige verwerking of verlies van persoonsgegevens af te handelen?

Ja, er is een calamiteitenplan/crisishandboek waarin procedures in geval van datalekken zijn opgenomen.

5. Hoe lang worden de persoonsgegevens bewaard? Geldt dezelfde bewaartermijn voor elk van de typen van verzamelde persoonsgegevens? Is het project onderworpen aan enige wettelijke/sectorale eisen met betrekking tot bewaring?

Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor het verwezenlijken van het doel van de verwerking. Contactgegevens van vaste aanspreekpunten voor het NCSC, zoals contactpersonen van vitale organisaties, worden bewaard voor zolang zij optreden als contactpersoon van die organisatie. De contactgegevens van andere personen die een melding hebben gedaan worden tot uiterlijk 13 maanden na het afhandelen van de melding bewaard, waarna deze zullen worden vernietigd. Andere persoonsgegevens, zoals bij het incident betrokken IP-adressen, zullen tot uiterlijk 18 maanden na afhandeling van het incident worden bewaard, waarna deze worden vernietigd. Als het NCSC gegevens ontvangt die niet strikt noodzakelijk zijn voor het uitvoeren van zijn taken, worden die zo spoedig mogelijk vernietigd.

6. Op welke beleidsmatige en technische gronden is deze termijn van bewaring vereist?

Deze bewaartermijnen zijn gebaseerd op de blijkens de huidige NCSC-praktijk gemiddeld benodigde maximale termijn om de NCSC-taken naar behoren te kunnen vervullen. Zo moet ook na enige tijd nog contact kunnen worden gezocht met de melder, bijvoorbeeld voor opvolging (hoe staat het er nu voor? heeft de bij het incident betrokken aanbieder het NCSC-advies gevolgd of zijn er andere maatregelen getroffen?) of om hem te waarschuwen voor kwetsbaarheden die zijn systeem opnieuw in gevaar kunnen brengen. Andere persoonsgegevens in voormelde zin (bijv. IP-adressen) kunnen van belang zijn als bijvoorbeeld blijkt dat een bepaald IP-adres opnieuw geraakt wordt of een digitale aanval steeds vanuit dezelfde hoek komt. Dit kan voor het NCSC aanleiding zijn om te onderzoeken of de aanval ook relevant is voor andere recent getroffen IP-adressen. Ook kan uit nieuw onderzoek van een afgehandeld incident blijken dat relevante informatie, zoals een kwetsbaarheid van bepaalde IP-adressen of een bepaalde aanvalstechniek, over het hoofd is gezien.

De bewaartermijnen zullen geregeld opnieuw worden beoordeeld en zullen dan zo mogelijk worden verkort en zo nodig worden verlengd. De huidige door het NCSC gehanteerde bewaartermijnen komen overigens overeen met de internationaal door CERT's gehanteerde termijnen.

7. Welke maatregelen zijn voorzien om de persoonsgegevens na afloop van de bewaartermijn te vernietigen? Worden alle persoonsgegevens, inclusief log-gegevens, vernietigd? Is er controle op de vernietiging, en door wie?

Het vernietigen van persoonsgegevens is onderdeel van de werkprocessen van het NCSC.

V. Transparantie en rechten van betrokkenen

1. **Is het doel van het verwerken van de gegevens bij de betrokkenen bekend of kan het bekend gemaakt worden? Wat is de procedure om betrokkenen indien nodig te informeren over het doel van de verwerking van hun persoonsgegevens?**

Wanneer het gaat om contactgegevens van de melder is het voor deze betrokkene bekend met welk doel zijn persoonsgegevens door het NCSC worden verwerkt. Dit is ook kenbaar op grond van de tekst van de wet.

Andere betrokkenen worden niet uit eigen beweging door het NCSC geïnformeerd over de verwerking van hen betreffende persoonsgegevens door het NCSC, daar dit een onevenredige inspanning van het NCSC zou vereisen (artikel 34 lid 4 Wbp).

2. **Indien u de persoonsgegevens direct van de betrokkenen verkrijgt, hoe stelt u hen van uw identiteit en het doel van de verwerking op de hoogte vóór het moment van verwerking?**

Het NCSC verkrijgt alleen persoonsgegevens direct van betrokkenen in het geval deze betrokkene een melding van een incident of inbreuk doet bij het NCSC. In dat geval verstrekt de betrokkene zelf zijn persoonsgegevens aan het NCSC. Op dat moment is de betrokkene zich bewust van het doel voor de verwerking van diens persoonsgegevens.

3. **Indien u de persoonsgegevens via een andere (overheids)organisatie verkrijgt, hoe zullen de betrokkenen van uw identiteit en het doel van de verwerking op de hoogte worden gesteld op het moment van verwerking?**

Andere betrokkenen dan de melder worden niet door het NCSC geïnformeerd over de verwerking van hen betreffende persoonsgegevens door het NCSC, daar dit een onevenredige inspanning van het NCSC zou vereisen (artikel 34 lid 4 Wbp).

4. **Indien u toestemming tot verwerking van persoonsgegevens aan de betrokkene vraagt (opt-in), kan de betrokkene deze toestemming dan op een later tijdstip weer intrekken (opt-out)? Bij een weigering toestemming te geven, of bij een dergelijke intrekking, wat is dan de implicatie voor de betrokkene?**

Niet van toepassing.

5. **Via welke procedure hebben betrokkenen de mogelijkheid zich tot de verantwoordelijke te wenden met het verzoek hen mede te delen of hun persoonsgegevens worden verwerkt? Hoe worden derden, die mogelijk bedenkingen hebben tegen een dergelijke mededeling, in de gelegenheid gesteld hun zienswijze te geven?**

Dit gebeurt op een ad-hoc-basis.

6. **Hoe kan een verzoek van een betrokkene tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens in behandeling worden genomen?**

Dit gebeurt op een ad-hoc-basis.