ONDERWERP : Motivering Risicoclassificatie overstapdossier

DATUM : 27 september 2011

De Stuurgroep dient als Verantwoordelijke in de zin van de Wet Bescherming Persoonsgegevens een besluit te nemen over de classificering van de verwerking van leerlinggegevens in het overstapdossier.

Vanwege het feit dat er in het overstapdossier enkele categorieën persoonsgegeven worden verwerkt die als gevoelig in de zin van de WBP dienen te worden aangemerkt, is de vraag aan de orde of de verwerkingen van de leerlinggegevens in het overstapdossier geplaatst moeten worden in Risicoklasse II dan wel Risicoklasse III, de hoogste risicoklasse.

In deze notitie wordt, ten behoeve van de besluitvorming door uw stuurgroep ten aanzien van de risicoklasse met betrekking tot de verwerking van leerlinggegevens in het overstapdossier,

1. geadviseerd om **Risicoklasse II** als een als een adequaat beschermingsniveau conform de Wet Bescherming Persoonsgegevens aan te merken;
2. gemotiveerd waarom het aanmerken van de verwerkingen als vallend in Risicoklasse II naar mijn mening als adequaat is aan te merken, alsmede
3. nader aangeduid welke zorgvuldige afwegingen leiden tot het aanmerken van Risicoklasse II als adequaat.

Motivering Klasse II adequaat beschermingsniveau

In deze motivering komen achtereen volgens aan de orde:

1. **Beveiliging - (Risico)classificatie van gegevens**
2. **Beveiliging - maatregelen voor gegevensuitwisseling**
3. **Taken Traffic Center**

Ad 1 - Beveiliging – (Risico)classificatie van gegevens
Deze alinea gaat over de Risicoklasse van de gegevens. Allereerst wordt opgemerkt dat de gegevens initieel door het Project werden ingedeeld in Risicoklasse III, de hoogste Risicoklasse, op basis van het feit dat er, met name, gevoelige gegevens worden verwerkt. Nadere overweging, mede in aanmerking nemend de kosten van het hanteren van Risicoklasse III in relatie tot de specifieke risico's en de aard van de te verwerken gegevens, heeft echter geleid tot de conclusie dat het goed verdedigbaar is, de indeling in Risicoklasse II als adequaat aan te merken.

Bij de bepaling van de Risicoklasse spelen de artikelen 13 en 16 van de Wet Bescherming Persoonsgegevens (WBP) een rol, alsook wat is uitgewerkt in AV23 (Achtergrond studies en verkenningen 23, uitgave van de Registratiekamer, door G.W. van Blarkom en drs. J.J. Borking).

Naast voornoemde wettelijke regels en de uitwerking door de Registratiekamer heb ik bij de bepaling van classificatie van de risicoklasse betrokken:

- CBP Richtsnoer 2009 informatieplicht Basisscholen
- Brief CBP inzake Wetgevingsadvies passend onderwijs 9 juni 2011.

In het vervolg van dit hoofdstuk treft u de hiervoor genoemde teksten met aan met daarin een markering van de bij de overweging betrokken tekstgedeelten. De tekst van AV23 is niet integraal opgenomen, alleen pagina 28 wordt geciteerd. De volledige tekst van AV23 is beschikbaar via de link http://www.cbpweb.nl/downloads_av/av23.pdf

Artikel 13 WBP luidt:
De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de ***stand der techniek*** *en* ***de kosten van de tenuitvoerlegging****,* ***een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens*** *met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.*

Het vereiste niveau van beveiliging van persoonsgegevens zal afhangen van de Risicoklasse die waarin de verwerking. De bepaling van deze risicoklasse komt in AV23 in hoofdstuk 3 aan de orde. Wanneer de risico's van de verwerking zijn geschat, komen andere aspecten aan de orde, namelijk de in artikel 13 WBP vermelde stand der techniek en de kosten van de ten uitvoerlegging van de maatregelen (paragraaf 2.6: *Wat zijn passende maatregelen?*). Deze risico's zijn van invloed op de mate waarin maatregelen en procedures moeten worden getroffen.

Bij de schriftelijke behandeling van de WBP in de Eerste Kamer werd door de minister van Justitie het volgende antwoord gegeven op de vraag, welke maatregelen nu als passend kunnen worden beschouwd:

'er kunnen geen algemene uitspraken worden gedaan over wat als een "passende beveiligingsmaatregel" kan worden beschouwd. Dit is namelijk afhankelijk van een aantal factoren. Het begrip "passend" duidt er op dat de maatregelen in overeenstemming dienen te zijn met de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. Met andere woorden de te nemen maatregelen moeten worden afgestemd op de ***risico's*** *van onrechtmatige verwerking die zich in de betrokken organisatie voordoen, waarbij tevens rekening dient te worden gehouden met de stand van de techniek en de kosten om de betrokken maatregelen ten uitvoer te brengen. Dit criterium moet in het licht van de concrete omstandigheden worden ingevuld en is voor een deel dynamisch.* ***Het vereiste niveau van bescherming is hoger naarmate er meer mogelijkheden voorhanden zijn om dat niveau te waarborgen****. Naarmate de gegevens een* ***gevoeliger karakter*** *hebben, of gezien de* ***context*** *waarin ze gebruikt worden een* ***groter risico voor de persoonlijke levenssfeer*** *van betrokkenen inhouden, dienen* ***zwaardere eisen aan de beveiliging*** *van die gegevens te worden gesteld.*
In het algemeen kan worden gesteld dat indien met naar verhouding geringe extra kosten meer beveiliging kan worden bewerkstelligd deze als "passend" moeten worden beschouwd, terwijl ***kosten die disproportioneel*** *zijn aan de* ***extra beveiliging*** *die daardoor zou worden verkregen,* ***niet worden vereist****. Met de zich ontwikkelende techniek zal periodiek een nieuwe afweging moeten worden gemaakt.'*

Bij het maken van de keuzes dient de verantwoordelijke te **zoeken naar een balans** tussen de benoemde criteria. Indien er met inachtneming daarvan een **gemotiveerde keuze** is gemaakt, is er sprake van een stelsel van passende technische en organisatorische maatregelen. Bij twijfel dient de **vastgestelde risicoklasse sturend** te zijn.

Artikel 16
De invloed die de **aard** van de persoonsgegevens in combinatie met de **omvang**, het **doel**, het **gebruik** en de verwerking kan hebben **op de positie van een betrokkene in de maatschappij**,

bepaalt mede welke eisen aan de beveiliging van persoonsgegevens dienen te worden gesteld.
In artikel 16 WBP wordt een aantal soorten persoonsgegevens aangeduid als zogenaamde "bijzondere persoonsgegevens": De verwerking van persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging is verboden behoudens het bepaalde in deze paragraaf. Hetzelfde geldt voor strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

CBP Richtsnoer uit 2009 Informatieplicht Basisscholen
http://www.cbpweb.nl/downloads_rs/rs_20090609_informatieplicht_basisscholen.pdf

De basisschool is volgens artikel 42 Wet op het primair onderwijs verplicht een onderwijskundig rapport op te stellen over iedere leerling die de school verlaat, onder wie leerlingen die naar een school voor voortgezet onderwijs gaan, en een afschrift daarvan aan zijn/haar ouders te verstrekken. In het onderwijskundig rapport worden persoonsgegevens vastgelegd en ook zaken die van invloed kunnen zijn op de prestaties in het voortgezet onderwijs (bijvoorbeeld **concentratie- en gezondheidsproblemen**).
http://www.cbpweb.nl/Pages/adv_z2003-0284.aspx en http://www.cbpweb.nl/downloads_adv/z2003-0284.pdf

Gelet op de toelichtende stukken bij het voorstel WBP moet er naar het oordeel van het CBP van worden uitgegaan dat **gegevens over IQ en sociaal-emotionele problematiek**, in elk geval bij een groot deel van de relevante doelgroep, **zijn aan te merken als persoonsgegevens over iemands gezondheid**.

Brief CBP inzake Wetgevingsadvies passend onderwijs 9 juni 2011
Inhoud wetsvoorstel
Het wetsvoorstel betreft wijzigingen van een aantal onderwijswetten in verband met de herziening van de organisatie en financiering van de leerlingenzorg in het primair onderwijs, het (voortgezet) speciaal onderwijs, het voortgezet onderwijs en het beroepsonderwijs. Er wordt een zorgplicht voor leerlingen met een specifieke onderwijsbehoefte voor de bevoegde gezagsorganen in het funderend onderwijs ingevoerd, er worden samenwerkingsverbanden in het funderend onderwijs gevormd, de zorgmiddelen voor het funderend onderwijs, het (voortgezet) speciaal onderwijs en het middelbaar beroepsonderwijs worden gebudgetteerd en tot slot wordt een verplichting tot overleg over de zorgvoorzieningen in het samenwerkingsverband tussen scholen en gemeenten ingesteld.
http://www.cbpweb.nl/downloads_adv/z2011-00468.pdf

" Het CBP adviseert de grondslag voor de *verwerking van gezondheidsgegevens* door Samenwerkingsverbanden in het licht van bovengenoemde opmerking nader te beschouwen."
Met zoveel woorden wordt er ook in het kader van deze nieuwe wetgeving van uit gegaan, dat er (onder meer) sprake is van het **verwerken van gezondheidsgegevens** door scholen.

Conclusie
- *Gesteld kan worden dat de conclusie inderdaad gerechtvaardigd is dat er in ieder geval gegevens zullen worden verwerkt, die kwalificeren als gezondheidsgegevens in de zin van de WBP.*
- *Dit blijkt ook uit de Datadictionary, met name de hierna volgende gegevens:*

Diagnose
De naam van de diagnose * **dyslexie, dyscalculie, dysfasie, dyspraxie, dysorthografie, NLD, ADHD, POD-NOS, Asperger, Gilles de la Tourette*
De naam van de diagnose
Vastgesteld door welke persoon
Deze persoon werkt bij instantie
Onderzoeksdatum
Onderwijsbelemmering
Extra hulp geboden in groep 7 of 8
Op welk gebied
Is het noodzakelijk om deze hulp voort te zetten
Is speciale begeleiding verleend
Welke soort begeleiding heeft plaatsgevonden
Moet speciale begeleiding voortgezet worden
Datum van aanvang van de Ambulante begeleiding
Verwijsindex risico jongeren
De leerling is ingevoerd in de Verwijsindex risicojongeren
Reden waarom de leerling is ingevoerd
Zorg Advies Team
Leerling is besproken in Zorg Advies Team
Reden waarom de leerling is besproken
Contact met Overige Instanties
De naam van de instelling, waarmee contact is geweest in verband met de leerling
De naam van de contactpersoon van die instelling
Arts
Soort arts
Persoonsgegevens

Op pagina 29 van de Algemene verkenning wordt een schema aangegeven, dat risicoklasse III van toepassing is, indien:

- Er sprake is van Bijzondere persoonsgegevens (artikel 16: o.a. gezondheidsgegevens)
- Er sprake is van de verwerking van veel persoonsgegevens

Gezien de tekstuele motivatie die op pagina 28 van hetzelfde document is gegeven, kan gesteld worden dat:

- Het schema op zichzelf niet volledig bepalend is/hoeft te zijn, maar op het schema een nuancering aangebracht kan worden met inachtneming van de (uitleg van) de wettelijke bepalingen en de tekstuele uitleg in hetzelfde rapport (zie hieronder), alsmede de hierboven genoemde documenten afkomstig van het CBP.

het beperken tot Risicoklasse II in plaats van Risicoklasse III op zichzelf in het geheel niet onlogisch voorkomt, gezien het zeer bijzondere karakter van de gegevens die in de hoogste klasse III dienen te vallen.Immers, ook risicoklasse II vereist al een hoger beveiligingsniveau.

Tevens moeten daarbij de kosten die gemoeid zijn met het hanteren van risicoklasse 3 versus risicoklasse 2 in achtgenomen worden. Als deze buitensporig veel hoger zijn, dan wordt het hanteren van risicoklasse III niet vereist. Hieronder volgt een samenvatting van de tekst t.a.v. de risicoklassen.

TEKST PAGINA 28

Risicoklasse 0: Publiek niveau
--
Risicoklasse I: Basis niveau
De risico's voor de betrokkene bij verlies of onbevoegd of onzorgvuldig gebruik van de persoonsgegevens zijn zodanig dat standaard (informatie)beveiligingsmaatregelen toereikend zijn. Bij verwerkingen van persoonsgegevens in deze klasse gaat het meestal om een beperkt aantal persoonsgegevens dat betrekking heeft op bijvoorbeeld lidmaatschappen, arbeidsrelaties, klantrelaties en overeenkomstige relaties tussen een betrokkene en een organisatie.
Voorbeelden van relaties waarover veelal persoonsgegevens worden verwerkt die vallen in deze klasse zijn: school - leerling, verhuurder - huurder, hotel - gast, vereniging - lid, organisatie - deelnemer.
Opgemerkt wordt dat het lidmaatschap van een instelling op zich al informatie kan bevatten betreffende een persoon. Indien dit gegevens zijn die vallen onder de categorie bijzondere gegevens, bijvoorbeeld over politieke voorkeur, seksuele leven, kerkelijk genootschappen etc., dan dient de beveiliging van persoonsgegevens tenminste te worden ondergebracht in risicoklasse II.

Risicoklasse II: Verhoogd risico
De uitkomst van de analyse toont aan dat er extra negatieve gevolgen bestaan voor de betrokkene bij verlies, onbehoorlijke of onzorgvuldige verwerking van de persoonsgegevens. De te nemen informatie) beveiligingsmaatregelen moeten voldoen aan hogere normen dan die gelden voor het basis niveau.
In deze klasse passen bijvoorbeeld verwerkingen van persoonsgegevens die voldoen aan een van de hieronder gegeven beschrijvingen:
1. de verwerkingen van bijzondere persoonsgegevens zoals bedoeld in artikel 16 WBP;
2. de verwerking in het bank- en verzekeringswezen van gegevens over de persoonlijke of economische situatie van een betrokkene;
3. de gegevens die bij handelsinformatiebureaus worden verwerkt ten behoeve van kredietinformatie of schuldsanering;
4. de gegevens die worden verwerkt hebben betrekking op de gehele of grote delen van de bevolking (de impact van op zich onschuldige gegevens over een groot aantal betrokkenen);
5. alle verwerkingen van persoonsgegevens die met het bovenstaande vergelijkbaar zijn.

Soms moet de verwerking van bijzondere gegevens vanwege een **hoge gevoeligheidsgraad i**n het maatschappelijk verkeer, **bijvoorbeeld** wanneer het gegevens over **levensbedreigende ziektes** betreft, ondergebracht worden in **Risicoklasse III**.

Risicoklasse III: Hoog risico
Bij verwerking van meerdere verzamelingen van bijzondere persoonsgegevens **kan** het resultaat van deze verwerking een **dermate** vergroot risico voor de betrokkene opleveren dat het **gerechtvaardigd is** deze verwerking van persoonsgegevens in risicoklasse III te plaatsen. De maatregelen die voor de beveiliging van dergelijke persoonsgegevens moeten worden genomen, **moeten voldoen aan de hoogste normen**. *De verwerking van persoonsgegevens die in deze klasse passen zijn onder andere de verwerkingen die betrekking hebben op opsporingsdiensten met bijzondere bevoegdheden of verwerkingen waarbij de belangen van de betrokkene ernstig kunnen worden geschaad indien dit onzorgvuldig of onbevoegd geschiedt. Bijzondere verwerkingen van persoonsgegevens, bijvoorbeeld een DNA-databank, vallen in deze klasse.*
Daarnaast valt de verwerking van persoonsgegevens waarop een bijzondere geheimhoudingsplicht van toepassing is binnen deze klasse. Deze geheimhoudingsplicht kan zowel wettelijk of anderszins formeel zijn geregeld door de overheid of door een private organisatie zijn ingevoerd voor haar medewerkers.

Conclusie
Tot slot kom ik tot de conclusie dat het dan ook (onder inbreng van argumenten van onder meer kostenoverwegingen en eventuele bovenmatige inspanningen) gemotiveerd te verdedigen is dat Risicoklasse II een adequate risicoklasse is met betrekking tot de verwerking van de leerling gegevens in het overstapdossier.

Het kwalificeren van de verwerkingen onder risicoklasse III is weliswaar een veilige keuze, indien als uitgangspunt wordt genomen "*better safe than sorry*". Maar indien de maatregelen die Risicoklasse II goed worden uitgewerkt en geïmplementeerd, dan zal naar mijn inschatting geen extra risico op onevenredige schade ontstaan.

Als projectmanager stel ik voor om het beveiligingsbeleid in te doen richten op basis van de eisen die worden gesteld op basis van de classificering van de verwerkingen van de leerlinggegevens in het overstapdossier als vallend in Risicoklasse II.

Aan deze keuze ligt nog geen concreet uitgewerkte vergelijking op basis van kosten en impact van het kwalificeren van klasse III boven II ten grondslag. Om definitief vast te stellen of deze kosten en impact feitelijk daadwerkelijk zodanig buitensporig zijn, dat dit niveau redelijkerwijs niet direct gekozen hoeft te worden, zouden deze nader onderzocht en vastgesteld dienen te worden.

Echter, op basis van de informatie* opgenomen in de bijlage, over het verschil in impact tussen de verschillende Risicoklassen I, II, en III, wordt na bestudering duidelijk dat de extra kosten van het kwalificeren van de gegevensverwerkingen in Risicoklasse III, boven de kosten die het hanteren van Risicoklasse II met zich mee zullen brengen, aanzienlijk zullen zijn door de maatregelen die met het classificeren in de verschillende Risicoklassen gemoeid zijn.

Ad 2 - Beveiliging - maatregelen voor gegevensuitwisseling
De reactie op dit onderdeel wil ik beginnen met een tweetal citaten uit het document AV23 en daarop een reactie geven.

Pagina 45: "*Een sterk aanbevolen maatregel voor het beveiligen van de datacommunicatie van persoonsgegevens is het versleutelen van berichten (encryptie). Hierdoor kan in ieder geval worden voorkomen dat berichten met persoonsgegevens zonder expliciet, bewust handelen ongeoorloofd worden gelezen door onbevoegde personen*".

Mijn mening is dat de verbinding op adequate wijze beveiligd dient te zijn. Het versleutelen van data levert technische bezwaren op die gelegen zijn in het versleutelen en ontsleutelen van de data op locatie, zowel bij de verzender als de ontvanger. Dit levert een te moeilijk te beheren hoeveelheid sleutelmateriaal op, voor welke optie als alternatief een goede encryptie op netwerkniveau naar mijn mening, na afweging van de extra kosten van versleuteling en ontsleuteling van data op locatie, tegenover de risico's samenhangend met de aard van de te verwerken gegevens, als adequaat kan worden beschouwd.

Pagina 46: "*Draadloze datacommunicatie geschiedt uitsluitend indien de persoonsgegevens versleuteld worden verzonden. Voor datacommunicatie via publieke netwerken, zoals internet, worden de persoonsgegevens op applicatieniveau, met algemeen erkende cryptografische methoden, versleuteld alvorens deze te verzenden. De gebruikte methoden en de sleutelprocedures dienen het risico van onbevoegde ontsleuteling uit te sluiten. De verzender van een bericht (systeem of gebruiker) vergewist zich ervan dat een getransporteerd bericht ongewijzigd is overgebracht*."

Ik ben van mening dat de beveiliging met certificaten zoals die is opgenomen in de documentatie juist is en passend voor de betreffende verwerkingen. De situatie rond beveiligingscertificaten zoals deze zich recentelijk heeft afgespeeld rondom de Diginotar zaak, leidt bij het te implementeren beveiligingsbeleid tot extra aandacht voor de keuze van de in te zetten certificaten, alsmede zwaardere eisen aan de leveranciers van de applicaties van leerling administratiegegevens ten aanzien van de beveiliging van de certificaten.

Tot slot van dit hoofdstuk merk ik op, dat de overstapdossiers rechtstreeks tussen de betreffende scholen worden uitgewisseld nadat in het proces is vastgesteld dat de verbinding met de juiste school is gemaakt.

Ad 3 - Traffic Center
Het traffic center heeft een centrale functie bij het beveiligd verzenden van de overstapdossiers. De nieuwe school die het overstapdossier opvraagt maakt eerst contact met het Traffic Center. De eerste controle die het traffic center uitvoert is de controle of de school waarbij het overstapdossier wordt opgevraagd gekwalificeerd is en of een er een ondertekende bewerkersovereenkomst bij de Raden aanwezig is. Als deze controle positief is ontvangt de vragende (nieuwe) school het technische adres van de huidige school en een sessie-ID. Met deze gegevens legt de nieuwe school contact met de huidige school. De huidige school legt vervolgens contact met het traffic center om het de sessie-ID te verifiëren. Als het ID juist is kan het overstapdossier uitgewisseld worden.
De contacten van de nieuwe en de huidige school met het traffic center zijn beveiligd met certificaten. In de aanvraag van het overstapdossier wordt het te verzenden leerlingnummer gecodeerd zodat het voor derden niet herkenbaar is.
Het traffic center verzorgt een logging van alle processen die door het traffic center worden uitgevoerd. Logging is op grond van de regelgeving een verplicht item. Naast het traffic center hebben de leerlingadministratiesystemen een belangrijke rol in het proces. Daar worden alle gegevens geregistreerd en beheert. Om vast te stellen dat het proces voldoende veilig wordt uitgevoerd zal het loggen van gegevens een onderdeel zijn van de kwalificatie van de leerlingadministratiesystemen.
.

Bijlage

Beveiligingsmaatregelen	Risicoklasse I	Risicoklasse II *Extra maatregelen boven klasse I*	Risicoklasse III *Extra maatregelen boven klasse II*
Beveiligingsbeleid, beveiligingsplan en implementatie van het stelsel van maatregelen en procedures	• Informatiebeveiligingsbeleid: definitie, organisatie, realisatieplicht, overdracht, instandhouding, onafhankelijke beoordeling, naleving • Implementatie: verankering, vaststellen dat beveiliging voldoet, frequenties controle, specialistisch advies, voldoende kennisniveau, communicatie, incidentmelding • Stelsel van maatregelen en procedures: beveiliging en verwerking conform beveiligingsbeleid en –plan, schriftelijk vastleggen, actualiseren, privacybewustzijn stimuleren, toezicht	• Aanpassen van beleid, implementatie en stelsel van maatregelen en procedures • Herstel van fouten.	• Aanpassen van beleid, implementatie en stelsel van maatregelen en procedures • Herstel van fouten.
Administratieve organisatie	• Richtlijnen AO rond beheer vastleggen • AO aanpassen na wijzigingen • Inrichting technische maatregelen sluit aan op organisatorische maatregelen • Verantwoordelijkheid expliciet toewijzen	• Taken, bevoegdheden en verantwoordelijkheden expliciet vastleggen • Functiescheiding • Beveiligingsfunctionaris.	• De inrichting van de organisatie voorziet in procedures om snel te kunnen reageren op ontwikkelingen die nieuwe maatregelen vereisen.
Beveiligingsbewustzijn	• Instructies alle medewerkers • Instructie gebruikers • Bij trainingen gebruik gegevens van niet bestaande personen • Disciplinaire maatregelen bij doorbreking geheimhoudingsplicht • Beveiliging ter sprake bij functioneringsgesprekken	• Verantwoordelijkheden beveiligen persoonsgegevens expliciet in arbeidscontract • Rapportageplicht beveiligingsincidenten • Bijscholing	• Verantwoordelijke medewerkers informeren management over niveau beveiligingsbewustzijn medewerkers • Tekenen geheimhoudingsverklaring bij indiensttreding
Eisen te stellen aan personeel	• Controleer CV sollicitant en vraag naar bewijsstukken • Controleer identiteit (Wet identificatieplicht)	• Tijdelijke medewerkers krijgen onder strikte, schriftelijk overeengekomen voorwaarden toegang tot verwerkingen van persoonsgegevens	• Verklaring omtrent gedrag • Referenties inwinnen • Betrouwbaarheids- of veiligheidsonderzoek

Inrichting werkplek	• Randapparatuur onder toezicht • Clean desk policy • Screensaver + wachtwoord + automatisch uitloggen	• Toegangscontrole voor mobiele apparatuur	• Uitsluitend goedgekeurde apparatuur • Markering van gegevensdragers
Beheer en classificatie van de ICT infrastructuur	• Verwerking aanmelden bij CBP of FG • Documentatie van datamodellen, software, datacommunicatieprotocollen • Overzicht van bevoegdheden	• Bij onderhoud aan apparatuur door derden moet de vertrouwelijke omgang met persoonsgegevens in het contract zijn vastgelegd. • Bij testen alleen gegevens fictieve personen	• Markeren van gegevensdragers
7. Toegangsbeheer en –controle	• Bevoegdheidsprofiel voor toegang opstellen • Bevoegdheden vastleggen • Bevoegdheden intrekken bij ontslag of wijziging functie • Alleen functionaliteit waarvoor bevoegdheid is verleend • Identiteit en authenticiteit gebruikers vaststellen • Tijdelijke wachtwoorden • Wachtwoorden nergens vastleggen • Maximaal 3x foutief wachtwoord	• Bij toegang via computernetwerk nauwkeurige identificatie • Directe melding bij overschrijding aantal toegestane inlogpogingen • Elke toegangspoging loggen • Bij het overdragen van bevoegdheden moet de rechtmatigheid ervan achteraf vastgesteld kunnen worden.	• Verboden bevoegdheden over te dragen • Het gebruik van controle op fysieke kenmerken als middel voor authenticatie van gebruikers dient te worden overwogen door middel van een kosten/baten analyse, daarbij rekening houdend met de ‘state of the art’.
Netwerken en externe verbindingen	• Vastleggen hoe datacommunicatie plaats moet vinden • Gebruik beveiligingsopties in aanwezige netwerkapparatuur en software • Firewalls bij toegang tot internet • Voorkom onbevoegde toegang via netwerkverbinding • Logische toegangsbeveiliging voor netwerkfaciliteiten	• Bij aanschaf apparatuur wordt aandacht geschonken aan beveiliging persoonsgegevens • Adequate fysieke beveiliging • De zend- en ontvangstpunten bij datacommunicatie verzekeren zich van elkaars juiste identiteit • Bij draadloze communicatie alleen versleutelde persoonsgegevens • Versleutelen van persoonsgegevens bij datacommunicatie via internet	• Datacommunicatie over netwerken buiten toezicht eigen organisatie alleen na expliciete waarborgen over beveiliging • Verzending van berichten loggen • Vergewissen dat bericht ongewijzigd is ontvangen

Gebruik van software van derden	• Maak gebruik van door verantwoordelijke goedgekeurde software • Rekening houden met beveiligingseisen bij aanschaf • Adequate administratie van versiebeheer	• Schriftelijke goedkeuring keuze software door verantwoordelijke • ESCROW overeenkomst bij software van derden	• 'Code review' bij toepassingssoftware
Bulkverwerking van persoonsgegevens	• Alleen door verantwoordelijke schriftelijk geautoriseerde versie van software • Aangeven welke persoonsgegevens, software, bestanden en verwerkingen • Procedures voor afhandeling van calamiteiten • Instructies vooraf expliciet vastleggen • Logbestanden bewaren • Logbestanden en processen alleen toegankelijk voor Bevoegden		
Bewaren van persoonsgegevens	• Zo bewaren dat alleen bevoegde personen over de gegevens beschikken • Geen gegevensdragers onbeheerd laten	• Gegevensdragers in afgesloten ruimte met inbraakdetectie bewaren	• Gemarkeerde gegevensdragers in inbraakwerende kluis bewaren • Persoonsgegevens op gegevensdragers zijn niet leesbaar voor onbevoegden
Vernietiging van persoonsgegevens	• Zorgvuldig vernietigen (geen persoonsgegevens achterlaten) • Toestemming verantwoordelijke nodig • Vernietiging van tussen- en testresultaten	• Administratie van vernietigde persoonsgegevens • Niet meer gebruikte gegevensdragers verlaten de organisatie alleen als de persoonsgegevens er op zijn vernietigd	
Calamiteitenplan	• Back-up voor elk bestand met persoonsgegevens • Back-up op andere locatie bewaren • Bewaartermijn voor back-up	• Back-up buiten de locatie bewaren	• Back-up voorzien van markering

Uitbesteden van en overeenkomsten voor de verwerking van persoonsgegevens	• Procedures rond autorisaties • Bijhouden logbestanden • Opslag gegevensdragers met persoonsgegevens • Verstrekken persoonsgegevens aan derden • Toereikend niveau van fysieke en logische beveiliging • Verantwoordelijke stelt zich op de hoogte van beveiligingsniveau	• Verantwoordelijke moet beveiligingsniveau bij bewerker (laten) controleren	• Alleen verwerking door bewerker als verantwoordelijke zich heeft verzekerd dat vereiste maatregelen zijn getroffen

* Gebaseerd op informatie afkomstig van TIAS - IT Auditing Tilburg Institute for Law, Technology and Society. Mr. Dr. Colette Cuipers