STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 5174
1 maart
2013

CBP Richtsnoeren: Beveiliging van persoonsgegevens

SAMENVATTING

Verantwoord omgaan met persoonsgegevens valt of staat met een adequate beveiliging van de gegevens. In de praktijk blijkt dat de aandacht voor beveiliging nogal eens tekortschiet. In de media zijn vrijwel dagelijks berichten te vinden over datalekken door onvoldoende beveiliging, waardoor persoonsgegevens op straat liggen. Het College bescherming persoonsgegevens (CBP) ontvangt ook regelmatig signalen over tekortschietende beveiliging en de kwalijke gevolgen ervan.

Beveiliging van persoonsgegevens is een van de speerpunten van het handhavingsbeleid van het CBP. Het CBP houdt toezicht op de naleving van de Wet bescherming persoonsgegevens (Wbp). Artikel 13 van de Wbp eist dat bedrijven en overheden die persoonsgegevens verwerken, 'passende technische en organisatorische maatregelen' nemen om persoonsgegevens te beveiligen.

Voldoen aan de wettelijke normen

Wanneer zijn beveiligingsmaatregelen nu 'passend' zoals de Wbp eist? Deze richtsnoeren leggen uit hoe het CBP bij het onderzoeken en beoordelen van beveiliging van persoonsgegevens in individuele gevallen de beveiligingsnormen uit de Wbp toepast. De richtsnoeren vormen de verbindende schakel tussen enerzijds het juridisch domein, met daarbinnen de eisen uit de Wbp, en anderzijds het domein van de informatiebeveiliging, waarin de noodzakelijke kennis en kunde aanwezig is om daadwerkelijk aan die eisen te voldoen.

Dat betekent dat de richtsnoeren in samenhang moeten worden gebruikt met algemeen geaccepteerde beveiligingsstandaarden binnen de praktijk van de informatiebeveiliging, zoals de Code voor Informatiebeveiliging of de ict-beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum.

Op tijd beginnen

Het uitgangspunt om tot een passende beveiliging te komen is dat in een organisatie bestuurders en de mensen die verantwoordelijk zijn voor de informatiesystemen en -beveiliging gezamenlijk nadenken over de wijze van beveiliging, al vóórdat ze persoonsgegevens gaan verzamelen. De beveiliging van persoonsgegevens binnen een organisatie moet gedurende de gehele levensduur van een informatiesysteem punt van aandacht zijn, van het allereerste ontwerp tot aan het onomkeerbaar wissen van het laatste back-up-bestand na afloop van de bewaartermijn. De beveiliging past binnen het bredere verband van *privacy by design*, waarbij de bescherming van persoonsgegevens en de borging van de rechten van de betrokkenen vanaf het allereerste begin in de informatiesystemen wordt ingebouwd.

'Plan-do-check-act'

Voor een blijvend passend beveiligingsniveau is inbedding van de zogeheten plan-do-check-act-cyclus in de dagelijkse praktijk van de organisatie noodzakelijk. Dat komt kort gezegd op het volgende neer:

1. *Beoordeel de risico's*
   Beoordeel de risico's die de gegevens en de aard van de verwerking met zich meebrengen voor de betrokkenen en bepaal op basis daarvan het gewenste beveiligingsniveau. Inventariseer vervolgens de dreigingen die kunnen leiden tot een beveiligingsincident, de gevolgen die het beveiligingsincident kan hebben en de kans dat deze gevolgen zich voor zullen doen. Tref op basis daarvan gericht beveiligingsmaatregelen die het gewenste beveiligingsniveau kunnen waarborgen.
2. *Maak gebruik van algemeen geaccepteerde beveiligingsstandaarden*
   Het vakgebied informatiebeveiliging kent vele beveiligingsmethoden, -standaarden en -maatregelen die zijn gebaseerd op ervaringen uit de dagelijkse beveiligingspraktijk. Gebruik bij het nemen van beveiligingsmaatregelen de richtsnoeren in samenhang met de beschikbare beveiligingsstandaarden. Deze standaarden geven houvast bij het daadwerkelijk treffen van passende maatregelen om de beveiligingsrisico's af te dekken.
3. *Controleer en evalueer regelmatig*
   Controleer met zekere regelmaat of de beveiligingsmaatregelen daadwerkelijk zijn getroffen en worden nageleefd. Beoordeel periodiek of het beveiligingsniveau nog steeds past bij de risico's die de verwerking en de aard van de te verwerken gegevens met zich meebrengen en of de beveili-

gingsmaatregelen nog steeds voldoen. Betrek daarbij ook de stand van de techniek en de nieuwste inzichten binnen het vakgebied informatiebeveiliging. Pas waar nodig de beveiligingsmaatregelen aan.

Tot slot

Met deze richtsnoeren wil het CBP duidelijk maken wat het van de beveiliging van persoonsgegevens verwacht. Daarbij heeft een organisatie de ruimte om de beveiliging van persoonsgegevens in te richten op de wijze en met de middelen die in de specifieke situatie van deze organisatie het meest passend zijn. Een organisatie dient hierbij altijd de rechten van de betrokkenen te waarborgen en er moet sprake zijn van adequate, vakkundig toegepaste beveiliging waarbij de organisatie optimaal benut wat het vakgebied informatiebeveiliging te bieden heeft.

INLEIDING

Iedereen moet erop kunnen vertrouwen dat zijn of haar persoonsgegevens voldoende worden beveiligd. Als dit niet zo is, kan dat leiden tot schade voor de betrokkenen (degenen op wie de persoonsgegevens betrekking hebben). Datalekken kunnen bijvoorbeeld tot gevolg hebben dat betrokkenen het slachtoffer worden van identiteitsfraude, oplichting of andere vormen van misbruik van hun persoonsgegevens. Ook als persoonsgegevens incorrect, verouderd of onvolledig zijn, kan dit de betreffende personen ernstig belemmeren in hun deelname aan het maatschappelijk leven. Een consequentie van het gebruik van foutieve of achterhaalde persoonsgegevens kan bijvoorbeeld zijn dat mensen geen toegang krijgen tot voorzieningen waar ze recht op hebben. Een van de belangrijkste doelstellingen van de beveiliging van persoonsgegevens is het voorkomen van dergelijke schade en waar deze zich toch voordoet, de gevolgen voor de betrokkenen zo veel mogelijk te beperken.

Het College bescherming persoonsgegevens (CBP) houdt toezicht op de naleving van de Wet bescherming persoonsgegevens (Wbp) en aanverwante wetten. Hoofdstuk 1 van deze richtsnoeren geeft de eisen weer die de Wbp stelt aan het beveiligen van persoonsgegevens. Hoofdstuk 2, 3 en 4 geven aan hoe het CBP de beveiliging van persoonsgegevens beoordeelt en hoofdstuk 5 gaat nader in op het toezicht door het CBP. Deze richtsnoeren dienen voor het CBP als uitgangspunt bij het onderzoeken en beoordelen van de beveiliging van persoonsgegevens en bij het toepassen van handhavende maatregelen.

De beveiliging van persoonsgegevens wordt in deze richtsnoeren in algemene zin beschreven, waarbij is aangesloten op standaarden, methoden en maatregelen die in het vakgebied informatiebeveiliging gebruikelijk zijn. In specifieke situaties kunnen organisaties ook met andere standaarden, methoden en maatregelen het vereiste beveiligingsniveau bereiken. Bij onderzoeken en beoordelingen van de beveiliging van persoonsgegevens zijn deze richtsnoeren voor het CBP evenwel het uitganspunt.

In deze richtsnoeren is een aantal praktijkvoorbeelden opgenomen. Deze praktijkvoorbeelden dienen uitsluitend ter illustratie. De voorbeelden gaan uit van de situatie bij het verschijnen van deze richtsnoeren en kunnen in de loop van de tijd door nieuwe ontwikkelingen worden achterhaald.

Deze richtsnoeren gelden voor verwerkingen van persoonsgegevens waarop de Wbp van toepassing is, zowel in de publieke als in de private sector. De richtsnoeren richten zich primair op de bestuurlijke verankering van de beveiliging van persoonsgegevens in organisaties. Bij het implementeren, controleren en evalueren van beveiligingsmaatregelen binnen een organisatie dient de organisatie deze richtsnoeren te gebruiken in samenhang met de algemeen geaccepteerde beveiligingsstandaarden die binnen het vakgebied informatiebeveiliging beschikbaar zijn.

Het beveiligen van persoonsgegevens is een van de verplichtingen die de Wbp oplegt aan verantwoordelijken voor de verwerking van persoonsgegevens. De beveiligingsmaatregelen die de verantwoordelijke treft, zijn onderdeel van het totaal aan maatregelen dat de verantwoordelijke neemt om te voldoen aan de Wbp. Bij de beoordeling van de rechtmatigheid van een verwerking spelen ook de overige bepalingen uit de Wbp een rol. Deze richtsnoeren gaan niet uitputtend in op deze andere bepalingen.

Behalve de Wbp kunnen op verwerkingen van persoonsgegevens nog andere wetten of regels van toepassing zijn. Voorbeelden van dergelijke regels zijn het Besluit voorschrift informatiebeveiliging rijksdienst 2007 (hierna: vir 2007)[1] en het Besluit voorschrift rijksdienst – bijzondere informatie (hierna:

[1] Stcrt. 2007, 122, p. 11. Het VIR 2007 geldt voor de ministeries met de daaronder vallende diensten, bedrijven en instellingen.

vir-bi)[2]. Organisaties dienen bij de beveiliging van persoonsgegevens te voldoen aan alle wetten en regels die van toepassing zijn. Deze richtsnoeren gaan niet in op deze overige wet- en regelgeving.

De Registratiekamer, de voorloper van het CBP, bracht in 2001 een publicatie uit over de beveiliging van persoonsgegevens (hierna: a&v 23).[3] Deze richtsnoeren vervangen a&v 23.
a&v 23 schreef op basis van een risicoclassificatie beveiligingsmaatregelen voor. De risicoclassificatie was gebaseerd op de aard van de verwerkte persoonsgegevens in combinatie met de hoeveelheid verwerkte persoonsgegevens en de complexiteit van de verwerking. Een risicogerichte benadering, waarbij op basis van analyse van de risico's gericht beveiligingsmaatregelen worden getroffen, ontbrak. Als gevolg daarvan is a&v 23, in ieder geval waar het gaat om het concreet treffen van beveiligingsmaatregelen, in de loop der jaren steeds verder af komen te staan van de beveiligingspraktijk. In deze richtsnoeren is daarom gekozen voor een methodiek die aansluit bij de gangbare praktijk van de informatiebeveiliging en die verantwoordelijken de flexibiliteit biedt om die beveiligingsmaatregelen te treffen die in hun situatie het meest passend zijn.

Rechterlijke uitspraken kunnen naast wetswijzigingen, technische ontwikkelingen en praktijkervaringen aanleiding geven tot aanvulling of herziening van deze richtsnoeren. Het CBP herziet de richtsnoeren in ieder geval bij de invoering van de algemene verordening gegevensbescherming.[4]
Bij het opstellen van de richtsnoeren is overigens zo veel mogelijk rekening gehouden met de relevante bepalingen uit de verordening.

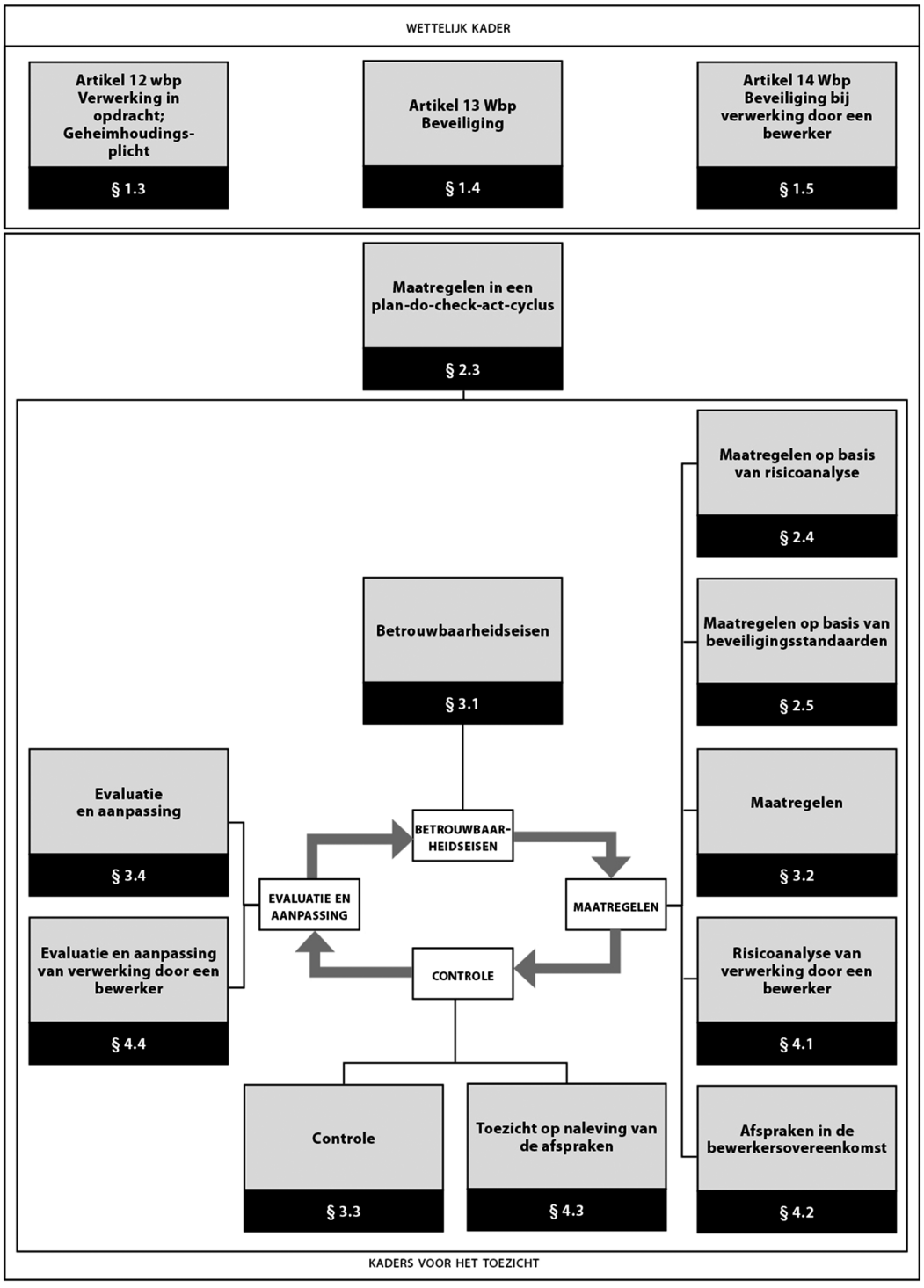
Deze richtsnoeren treden in werking met ingang van 1 maart 2013, zijnde de datum van publicatie in de Staatscourant.

[2] Stcrt. 2004, 47; rectificatie in Stcrt. 2004, 49. Het VIR-BI is een aanvulling op het VIR 2007 en is van toepassing op de beveiliging van informatie waarvan de kennisname door niet-gerechtigden schade of nadeel op kan leveren voor de staat, zijn bondgenoten of een of meer ministeries.

[3] G.W. van Blarkom en drs. J.J. Borking, 'Beveiliging van persoonsgegevens', *Achtergrondstudies en Verkenningen* nr. 23, Registratiekamer, april 2001 (http://www.cbpweb.nl/downloads_av/av23.pdf).

[4] De Europese Commissie stelt een nieuw regelgevend kader voor dat bestaat uit een algemene verordening bescherming persoonsgegevens en een richtlijn die betrekking heeft op de bescherming van persoonsgegevens die worden verwerkt in het kader van politiële en justitiële activiteiten. Meer informatie is beschikbaar op de website van de Eerste Kamer (http://www.eerstekamer.nl/eu/edossier/e120003_voorstel_voor_een) en op de website van de Europese Commissie (http://ec.europa.eu/justice/data-protection/).

SCHEMA BEVEILIGING VAN PERSOONSGEGEVENS



6 | CBP Richtsnoeren

1 BEVEILIGING IN DE WBP

Dit hoofdstuk gaat in op de wettelijke verplichting om persoonsgegevens te beveiligen zoals die is opgenomen in de Wet bescherming persoonsgegevens (Wbp). De eisen uit de Wbp die voor deze richtsnoeren relevant zijn staan in dit hoofdstuk weergegeven, voorzien van de relevante onderdelen

uit de memorie van toelichting bij de Wbp.[5]De volledige tekst van de geciteerde wetsartikelen is opgenomen in een bijlage bij deze richtsnoeren.

1.1 Achtergrond

De beveiliging van persoonsgegevens is onderdeel van de informationele privacy: de bescherming van de persoonlijke levenssfeer bij het verzamelen en verwerken van persoonsgegevens. De bescherming van de persoonlijke levenssfeer is een van de grondrechten van onze rechtsorde.[6] Sinds 2001 wordt hieraan uitvoering gegeven door de Wbp, die tevens de implementatie vormt van de Europese richtlijn 95/46/eg.

1.2 Begrippen uit de Wbp

Voor deze richtsnoeren zijn de volgende begrippen uit de Wbp relevant:
• *Persoonsgegevens*
Persoonsgegevens in de zin van de Wbp zijn alle gegevens "betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'.[7] Een persoon is identificeerbaar "indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden".[8, 9]
• *Verwerking*
Een verwerking van persoonsgegevens in de zin van de Wbp is "elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens".[10] Verwerkingen zijn "in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens".[11]
• *Verantwoordelijke*
De verantwoordelijke in de zin van de Wbp is degene die "het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt".[12] De verantwoordelijke bepaalt welke persoonsgegevens, voor welk doel, op welke manier en met welke middelen worden verwerkt.[13]
• *Betrokkene*
De betrokkene is degene "op wie een persoonsgegeven betrekking heeft"[14] of "waarover de gegevens informatie bevatten".[15]
• *Bewerker*
Bij de verwerking van persoonsgegevens kan de verantwoordelijke een bewerker inschakelen. "De bewerker is [...] een buiten de organisatie van de verantwoordelijke staande persoon of instelling".[16] Hij "bewerkt gegevens ten behoeve van de verantwoordelijke, dat wil zeggen overeenkomstig diens instructies en onder diens (uitdrukkelijke) verantwoordelijkheid".[17] De bewerker "beperkt [...] zich tot het verwerken van persoonsgegevens zonder zeggenschap te hebben over het doel van en de middelen voor de verwerking van persoonsgegevens. Hij neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens enz."[18]

1.3 Artikel 12 Wbp: verwerking in opdracht; geheimhoudingsplicht

Artikel 12 Wbp richt zich op de bewerker en op hen die onder het gezag van de verantwoordelijke of

---

5 In paragraaf 1.3, 1.4 en 1.5 worden de citaten uit de Wbp gecursiveerd weergegeven. De bijbehorende citaten uit de memorie van toelichting volgen direct na het betreffende citaat uit de Wbp.
6 Artikel 10 Grondwet; artikel 8 Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM); artikel 7 en 8 van het EU-Handvest voor de grondrechten.
7 Artikel 1 sub a Wbp.
8 Kamerstukken II 1997-1998, 25 892, nr. 3, p. 47.
9 De Europese toezichthouders op de gegevensbescherming hebben in 2007 een advies gepubliceerd over het begrip 'persoonsgegevens', waarin het begrip uitgebreid en voorzien van voorbeelden wordt toegelicht. Groep gegevensbescherming artikel 29 (WP 29), *Advies 4/2007 over het begrip persoonsgegevens*, goedgekeurd op 20 juni 2007 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_nl.pdf).
10 Artikel 1 sub b Wbp.
11 Artikel 1 sub b Wbp.
12 Artikel 1 sub d Wbp.
13 De Europese toezichthouders op de gegevensbescherming hebben in 2010 een advies gepubliceerd over de begrippen 'verantwoordelijke' en 'bewerker', waarin deze beide begrippen uitgebreid en voorzien van voorbeelden worden toegelicht. WP29, *Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker"*, goedgekeurd op 16 februari 2010 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_nl.pdf).
14 Artikel 1 sub f Wbp.
15 Kamerstukken II 1997-1998, 25 892, nr. 3, p. 63.
16 Kamerstukken II 1997-1998, 25 892, nr. 3, p. 61.
17 Kamerstukken II 1997-1998, 25 892, nr. 3, p. 61.
18 Kamerstukken II 1997-1998, 25 892, nr. 3, p. 61-62.

de bewerker werkzaam zijn. Zij verwerken uitsluitend persoonsgegevens in opdracht van de verantwoordelijke:

"Een ieder die handelt onder het gezag van de verantwoordelijke of van de bewerker, alsmede de bewerker zelf, voor zover deze toegang hebben tot persoonsgegevens, verwerkt deze slechts in opdracht van de verantwoordelijke, behoudens afwijkende wettelijke verplichtingen."[19]

"Het uitgangspunt is dat de verantwoordelijke verantwoordelijk en aansprakelijk is voor de gegevensverwerking. Deze verantwoordelijkheid kan hij slechts dragen wanneer zijn ondergeschikten of degenen die in opdracht van de verantwoordelijke gegevens verwerken, zich naar zijn aanwijzingen richten."[20]

Verder wordt aan hen een geheimhoudingsplicht opgelegd:

"De personen, bedoeld in het eerste lid, voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit."[21]

"[Deze] bepaling legt een geheimhoudingsplicht op aan de bewerker, alsmede degenen die onder het gezag van de verantwoordelijke of de bewerker werkzaam zijn. In beginsel kan slechts een uitdrukkelijke wettelijke verplichting op de geheimhoudingsplicht een inbreuk maken."[22]

1.4 Artikel 13 Wbp: beveiliging

De verantwoordelijke treft passende beveiligingsmaatregelen:

"De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking."[23]

"Onder onrechtmatige vormen van verwerking vallen de aantasting van de gegevens, onbevoegde kennisneming, wijziging, of verstrekking daarvan."[24]

De maatregelen garanderen een passend beveiligingsniveau:

"Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico"s die de verwerking en de aard van te beschermen gegevens met zich meebrengen."[25]

"In het begrip 'passend' ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. [...] Het begrip 'passend' duidt mede op een proportionaliteit tussen de beveiligingsmaatregelen en de te beschermen gegevens. Naarmate bijvoorbeeld de gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden zwaardere eisen gesteld aan de beveiliging van de gegevens. Er is geen verplichting om steeds de allerzwaarste beveiliging te nemen. Daarom duidt ook het feit dat inbreuken zijn gemaakt op het beveiligingsniveau niet noodzakelijkerwijs op nalatigheid in de beveiliging.
Er moet sprake zijn van een adequate beveiliging."[26]
"Er kunnen geen algemene uitspraken worden gedaan over wat als een 'passende beveiligingsmaatregel' kan worden beschouwd. [...] 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. [...] 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 zich ontwikkelende techniek zal periodiek een nieuwe afweging moeten worden gemaakt."[27]

---

[19] Artikel 12 lid 1 Wbp.
[20] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 97.
[21] Artikel 12 lid 2 Wbp.
[22] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 97.
[23] Artikel 13 Wbp.
[24] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 98.
[25] Artikel 13 Wbp.
[26] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 99.
[27] Kamerstukken I 1999-2000, 25 892, nr. 92c, p. 15.

Voor de maatregelen geldt verder:

"Technische en organisatorische maatregelen dienen cumulatief te worden getroffen. Software is een belangrijk instrument tot beveiliging. [De Wbp] geeft de normen die mede met behulp van software dienen te worden gehandhaafd."[28]

Naast de beveiliging van persoonsgegevens ziet artikel 13 Wbp ook op de toepassing van *privacy enhancing technologies* (pet):

"De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen."[29]

"De beveiligingsverplichting die in dit artikel is opgenomen strekt zich uit tot alle onderdelen van het proces van gegevensverwerking. Juridische normen zullen moeten worden vertaald in de feitelijke inrichting en verdere ontwikkeling van informatiesystemen. Steeds meer zullen 'privacy enhancing technologies' (pet) daarvoor onmisbaar zijn. Door te eisen dat de inrichting van systemen mede gericht moet zijn op het voorkomen van onnodige verzameling en verdere verwerking van persoonsgegevens, wordt bewerkstelligd dat in plaats van een voortdurende controle op individuele gevallen van onrechtmatig gegevensgebruik het accent meer gelegd kan worden op de structuur van informatiesystemen."[30]

pet is de verzamelnaam voor een aantal technieken die de verantwoordelijke kan toepassen om bij het verwerken van persoonsgegevens de risico"s voor de betrokkenen te beperken. Een centraal principe van pet is het verminderen van de herleidbaarheid: de mate waarin persoonsgegevens kunnen worden herleid tot de betrokkenen.
De zwaarste vorm van pet is anonimisering van de verwerkte persoonsgegevens. Van anonimisering is sprake als de gegevens op geen enkele manier meer tot de betrokkene te herleiden zijn. Er is dan geen sprake meer van persoonsgegevens en de Wbp is niet meer van toepassing op de gegevens. Een lichtere vorm van pet is het scheiden van de verwerkte persoonsgegevens in (zeer goed beveiligde) identificerende gegevens en niet-identificerende gegevens. Alleen met behulp van de identificerende gegevens kan de identiteit van de betrokkenen worden achterhaald.[31]

1.5 Artikel 14 Wbp: beveiliging bij verwerking door een bewerker

Bij verwerking door een bewerker zorgt de verantwoordelijke voor voldoende waarborgen en ziet deze toe op naleving:

"Indien de verantwoordelijke persoonsgegevens te zijnen behoeve laat verwerken door een bewerker, draagt hij zorg dat deze voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen. De verantwoordelijke ziet toe op de naleving van die maatregelen."[32]

"De verantwoordelijke draagt zorg dat de bewerker
a. *de persoonsgegevens verwerkt in overeenstemming met artikel 12, eerste lid en*
b. *de verplichtingen nakomt die op de verantwoordelijke rusten ingevolge artikel 13."*[33]

"De strekking van de bepaling is te voorkomen dat bij eventuele tekortkomingen in de gegevensverwerking, verantwoordelijke en bewerker zich wat betreft hun verantwoordelijkheden achter elkaar zouden kunnen verschuilen. De verplichtingen moeten over en weer duidelijk zijn neergelegd. Op de verantwoordelijke rust een zorgplicht daarvoor zorg te dragen. Niet alleen dient hij civielrechtelijk de bewerker voldoende te hebben duidelijk gemaakt hoe met de persoonsgegevens wordt omgegaan, tevens dient hij toe te zien op de feitelijke naleving van de aldus gecreëerde verplichtingen."[34]

De te treffen beveiligingsmaatregelen worden vastgelegd in de bewerkersovereenkomst:

---

[28] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 99.
[29] Artikel 13 Wbp.
[30] Kamerstukken II 1999-2000, 25 892, nr. 22.
[31] Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft een publicatie uitgebracht waarin de toepassing van PET uitvoerig wordt toegelicht: Drs. ing. Ronald Koorn RE e.a., *Privacy enhancing technologies, Witboek voor beslissers*, ministerie van Binnenlandse Zaken en Koninkrijksrelaties, december 2004 (http://www.cbpweb.nl/downloads_technologie/witboek_pet.pdf).
[32] Artikel 14 lid 1 Wbp.
[33] Artikel 14 lid 3 Wbp.
[34] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 99.

"De uitvoering van verwerkingen door een bewerker wordt geregeld in een overeenkomst of krachtens een andere rechtshandeling waardoor een verbintenis ontstaat tussen de bewerker en de verantwoordelijke."[35]

"Met het oog op het bewaren van het bewijs worden de onderdelen van de overeenkomst of de rechtshandeling die betrekking hebben op de bescherming van persoonsgegevens, alsmede de beveiligingsmaatregelen als bedoeld in artikel 13 schriftelijk of in een andere, gelijkwaardige vorm vastgelegd."[36]

"De ratio is dat de betrokkene als een soort impliciete derde belanghebbende, in geval jegens hem onrechtmatig wordt gehandeld, over de nodige bewijsstukken kan beschikken wanneer deze overeenkomstig de regels van het procesrecht een rol gaan spelen. Klassiek zou daartoe een schriftelijke neerslag van de afspraken, van belang kunnen zijn. In de toekomstige informatiemaatschappij zijn ook andere, gelijkwaardige vormen van gegevensopslag denkbaar [...]."[37]

De bewerker kan bij de verwerking van persoonsgegevens een subbewerker inschakelen. Dit gebeurt uitsluitend met uitdrukkelijke instemming van de verantwoordelijke:

"Uit de verantwoordelijkheid van de opdrachtgever – die in de zin van de wet geldt als verantwoordelijke voor de gegevensverwerking – vloeit voort dat hij uitdrukkelijk heeft ingestemd met het subbewerkerschap. Indien de verantwoordelijke daarvoor in zijn overeenkomst met de bewerker uitdrukkelijk ruimte heeft gegeven, kan de bewerker – met behoud van zijn volle aansprakelijkheid voor de naleving van zijn contract met de verantwoordelijke – delen van de verwerking uitbesteden aan 'subbewerkers'."[38]

De door de subbewerker te treffen beveiligingsmaatregelen worden vastgelegd in de overeenkomst tussen de bewerker en de subbewerker en de verantwoordelijke wordt in staat gesteld om toe te zien op naleving:

"De bewerker dient [...] contractueel verzekerd te hebben dat de subbewerker zich eveneens richt naar de instructies van de verantwoordelijke, tot geheimhouding verplicht is en de nodige beveiligingsmaatregelen ten opzichte van de gegevensverwerking neemt. De verantwoordelijke dient hiervan wel op de hoogte te worden gesteld opdat deze in staat is toe te zien op de naleving van zijn afspraken met de bewerker."[39]

1.6 Beveiliging als onderdeel van privacy by design

De verantwoordelijke kan op de meest efficiënte en effectieve wijze aan de Wbp voldoen door al bij het ontwerp van de verwerking rekening te houden met de wettelijke eisen (privacy by design). De beveiliging van persoonsgegevens is een van de aspecten waarmee de verantwoordelijke bij de toepassing van privacy by design rekening moet houden. Andere aspecten zijn onder meer dataminimalisatie (het beperken van de verwerking van persoonsgegevens tot het hoogst noodzakelijke) en transparantie (het adequaat informeren van de betrokkenen over wat er met hun persoonsgegevens gebeurt). Deze aspecten van privacy by design vallen buiten het bereik van deze richtsnoeren.

1.7 De rol van de functionaris voor de gegevensbescherming (fg)

De Wbp geeft verantwoordelijken en brancheorganisaties de mogelijkheid om een interne toezichthouder aan te stellen: de functionaris voor de gegevensbescherming (fg).[40] Bij de beveiliging van persoonsgegevens kan deze een belangrijke rol spelen, onder meer bij de controle op naleving van beveiligingsmaatregelen (zie paragraaf 3.3 en 4.3 van deze richtsnoeren) en bij evaluatie en aanpassing van de beveiliging (zie paragraaf 3.4 en 4.4). Het is echter aan de organisatie en aan de fg zelf om hier invulling aan te geven.

2 HET VAKGEBIED INFORMATIEBEVEILIGING

De beveiliging van persoonsgegevens valt uiteen in twee aspecten: de bescherming van persoonsgegevens en het beveiligen van informatie. Dit hoofdstuk gaat in op het laatste. Het hoofdstuk richt zich met name op drie elementen uit het vakgebied informatiebeveiliging die het CBP

[35] Artikel 14 lid 2 Wbp.
[36] Artikel 14 lid 5 Wbp.
[37] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 100.
[38] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 63.
[39] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 63.
[40] Artikel 62, 63 en 64 Wbp.

beschouwt als randvoorwaarden om tot passende maatregelen te komen zoals de wet die voorschrijft: maatregelen treffen op basis van risicoanalyse, beveiligingsstandaarden toepassen en de inbedding in een plan-do-check-act-cyclus.

2.1 Achtergrond

Informatiebeveiliging omvat het geheel aan maatregelen waarmee organisaties hun informatie beveiligen. Het gaat daarbij om alle informatie die de organisatie verwerkt, zowel digitaal als niet-digitaal. Persoonsgegevens, zoals het klantenbestand en de personeelsadministratie, maken hier deel van uit. Organisaties hebben niet alleen informatie nodig om hun bedrijfsprocessen uit te voeren, maar ook om hun interne bedrijfsvoering bij te sturen en strategische beslissingen te nemen. De term 'informatiebeveiliging' wordt ook gebruikt voor het vakgebied dat zich bezighoudt met het beveiligen van informatie.

2.2 Begrippen uit het vakgebied informatiebeveiliging

Een centraal begrip uit het vakgebied informatiebeveiliging is:
• *Betrouwbaarheid en betrouwbaarheidseisen*
Betrouwbaarheid is de mate waarin een organisatie voor de informatievoorziening kan rekenen op een informatiesysteem. De betrouwbaarheid van een informatiesysteem is de verzamelterm voor drie aspecten van beveiliging die binnen het vakgebied informatiebeveiliging algemeen zijn geaccepteerd: beschikbaarheid, integriteit en vertrouwelijkheid. De betrouwbaarheidseisen geven weer aan welke eisen het informatiesysteem moet voldoen met betrekking tot deze drie aspecten.

De hierboven genoemde aspecten beschikbaarheid, integriteit en vertrouwelijkheid worden binnen het vakgebied informatiebeveiliging als volgt gedefinieerd:
• *Beschikbaarheid*
Beschikbaarheid betreft het waarborgen dat geautoriseerde gebruikers op de juiste momenten toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen).
• *Integriteit*
Integriteit betreft het waarborgen van de juistheid, tijdigheid (actualiteit) en volledigheid van informatie en de verwerking ervan.
• *Vertrouwelijkheid*
Met vertrouwelijkheid wordt gedoeld op het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd.
Naast de drie bovengenoemde aspecten, die betrekking hebben op de informatie en de verwerking ervan, wordt nog een vierde aspect onderkend:
• *Controleerbaarheid*
Controleerbaarheid betreft de mogelijkheid om met voldoende zekerheid vast te kunnen stellen of wordt voldaan aan de eisen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid.

Het begrip 'betrouwbaarheid' uit het vakgebied informatiebeveiliging komt overeen met het begrip 'beveiligingsniveau' dat in de memorie van toelichting bij de Wbp wordt gehanteerd, met daarbij de kanttekening dat het aspect 'beschikbaarheid' deels buiten de reikwijdte van artikel 13 Wbp valt.

Het begrip 'beschikbaarheid' uit het vakgebied informatiebeveiliging valt uiteen in twee aspecten:
- Het waarborgen dat informatiesystemen op de juiste momenten beschikbaar zijn voor de gebruiker, bijvoorbeeld door extra machinecapaciteit in te zetten, zodat bedrijfskritische informatiesystemen 7 dagen per week, 24 uur per dag gebruikt kunnen worden. Dit aspect valt buiten de reikwijdte van artikel 13 Wbp.
- Het beveiligen van gegevens tegen verlies, waarbij onder 'verlies' het definitief verloren gaan van de gegevens wordt verstaan. Bedrijfscontinuïteitsbeheer is mede gericht op dit aspect.[41] Dit aspect komt overeen met het "beveiligen tegen verlies" uit artikel 13 Wbp.

Het begrip 'integriteit' komt binnen de context van de beveiliging van persoonsgegevens overeen met de beveiliging tegen "aantasting van de gegevens [of onbevoegde wijziging]"[42] uit de Wbp.

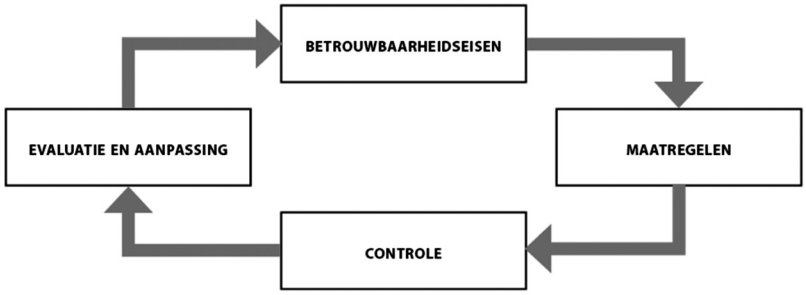
Het begrip 'vertrouwelijkheid' komt overeen met de beveiliging tegen "onbevoegde kennisneming [...] of verstrekking"[43] uit de Wbp.

[41] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 14.
[42] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 98.
[43] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 98.

2.3 Maatregelen in een plan-do-check-act-cyclus

Inbedding van de plan-do-check-act-cyclus of kwaliteitscirkel in de dagelijkse praktijk van de organisatie stelt de verantwoordelijke in staat om tot een blijvend passend beveiligingsniveau te komen.

Het onderstaande schema geeft deze cyclus weer.



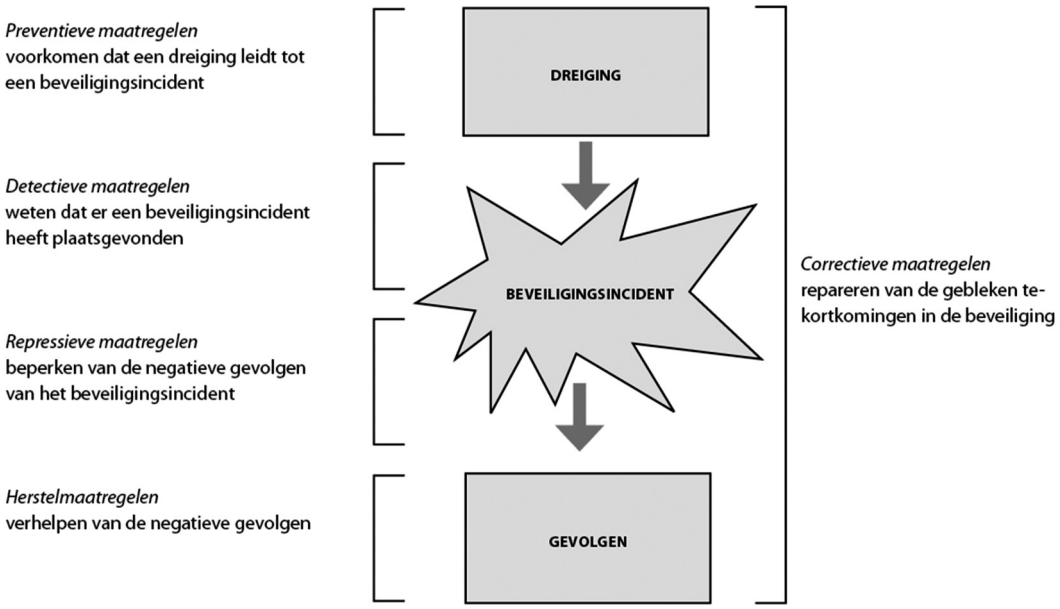
Na het vaststellen van de betrouwbaarheidseisen treft de verantwoordelijke maatregelen waarmee hij waarborgt dat aan de betrouwbaarheidseisen wordt voldaan. Vervolgens controleert de verantwoordelijke of de maatregelen daadwerkelijk getroffen zijn en het gewenste effect sorteren. Het totaal aan betrouwbaarheidseisen, maatregelen en controle wordt regelmatig geëvalueerd en waar nodig aangepast, waardoor een blijvend passend beveiligingsniveau wordt bereikt.

De volgende paragrafen gaan nader in op twee elementen die het CBP beschouwt als noodzakelijke randvoorwaarden om tot passende maatregelen te komen: het treffen van maatregelen op basis van risicoanalyse en het toepassen van beveiligingsstandaarden. De risicoanalyse geeft aan welke risico"s moeten worden afgedekt om aan de betrouwbaarheidseisen te voldoen. Beveiligingsstandaarden geven aan welke maatregelen daarbij ter beschikking staan.

2.4 Maatregelen op basis van risicoanalyse

Het treffen van maatregelen op basis van een risicoanalyse stelt de verantwoordelijke in staat om passende maatregelen te treffen die een passend beveiligingsniveau garanderen.[44]

Onderstaand schema geeft de belangrijkste elementen uit de risicoanalyse weer, met daarbij de verschillende typen maatregelen die de verantwoordelijke kan treffen om de risico"s af te dekken.



[44] De relatie tussen de risicoanalyse zoals deze in de informatiebeveiliging gebruikelijk is en het *privacy impact assessment* (PIA) wordt toegelicht in de inleiding bij hoofdstuk 3 van deze richtsnoeren.

De verantwoordelijke inventariseert de dreigingen die kunnen leiden tot een beveiligingsincident, de gevolgen die dit incident kan hebben en de kans dat deze gevolgen zich voordoen. De dreigingen kunnen onder meer samenhangen met de specifieke kenmerken van de verwerking en de gebruikte technologie. Bij verwerking via internet is bijvoorbeeld hacking een dreiging waarmee rekening moet worden gehouden; bij verwerking op draagbare computers en opslag op draagbare geheugenmedia zijn vermissing en diefstal dreigingen die de verantwoordelijke in de risicoanalyse moet betrekken.
De verantwoordelijke treft maatregelen op basis van de uitgevoerde risicoanalyse en kiest de maatregelen zodanig dat wordt voldaan aan de vastgestelde betrouwbaarheidseisen.

Praktijkvoorbeeld: Hulp na datalek als voorbeeld van een herstelmaatregel

Onderstaand voorbeeld illustreert wat in het vakgebied informatiebeveiliging wordt verstaan onder een herstelmaatregel.

Hackers plegen twee grootschalige inbraken bij een grote fabrikant van spelcomputers en computerspellen en stelen daarbij de accountgegevens van meer dan honderd miljoen abonnees. Bij de inbraken zijn er mogelijk tien miljoen creditcardnummers buitgemaakt en hebben de hackers bovendien toegang gekregen tot een oude database met daarin de incassogegevens van ruim 10.000 mensen. De fabrikant besluit om ervoor te zorgen dat Amerikaanse abonnees eventuele schade als gevolg van identiteitsfraude door de inbraken vergoed krijgen tot een miljoen dollar per gebruiker. Voor dit doel maakt de fabrikant afspraken met een bedrijf dat gespecialiseerd is in het monitoren van identiteitsfraude.
Ook andere delen van de wereld krijgen een dergelijke regeling.

2.5 Maatregelen op basis van beveiligingsstandaarden

De risicoanalyse geeft aan welke risico"s moeten worden afgedekt; beveiligingsstandaarden geven houvast bij het daadwerkelijk treffen van passende maatregelen om de risico"s af te dekken. Veel beveiligingsstandaarden bevatten ook een 'basisset' aan maatregelen die in de meeste situaties noodzakelijk zijn om tot adequate beveiliging te komen.

Beveiligingsstandaarden vormen een weerslag van de *lessons learned* die bij de beveiliging in een specifieke branche of in een specifieke technologische omgeving zijn opgedaan. Ze geven weer welke maatregelen door beveiligingsdeskundigen binnen de betreffende context in het algemeen als 'passend' worden beschouwd en, in het geval van de meer technisch gerichte standaarden, welke technologische middelen bij de beveiliging worden toegepast. Er worden ook met grote regelmaat nieuwe beveiligingsstandaarden en nieuwe versies van bestaande beveiligingsstandaarden gepubliceerd, waarmee wordt aangesloten op de nieuwste ontwikkelingen binnen het vakgebied. Correct gebruik van actuele beveiligingsstandaarden stelt de verantwoordelijke in staat om passende maatregelen te treffen en om tot een evenwichtig en effectief geheel aan technische en organisatorische maatregelen te komen. Het vervolg van deze paragraaf licht het gebruik van standaarden toe aan de hand van concrete voorbeelden.

Een zeer veel gebruikte beveiligingsstandaard is de Code voor Informatiebeveiliging (nen-iso/iec 27002:2007 nl).[45] Deze standaard is onderdeel van een groep onderling samenhangende standaarden voor het initiëren, implementeren, handhaven en verbeteren van de informatiebeveiliging in een organisatie. Evenals de standaard nen-iso/iec 27001:2005 nl, die tot dezelfde groep behoort, is de Code voor Informatiebeveiliging opgenomen in de "lijst met open standaarden waarvoor voor overheidsorganisaties een 'pas-toe-of-leg-uit- regime' geldt"[46] van het College en Forum Standaardisatie.[47]
De Code voor Informatiebeveiliging is een technologieneutrale standaard die binnen de informatiebeveiliging breed wordt toegepast bij het formuleren en implementeren van beveiligingsmaatregelen. Daarom wordt in deze richtsnoeren, waar deze ingaan op concrete beveiligingsmaatregelen, verwezen naar de betreffende onderdelen van de Code voor Informatiebeveiliging. De relevante informatie is daarbij opgenomen in de tekst van de richtsnoeren.
Voor de zorgsector is de Code voor Informatiebeveiliging nader uitgewerkt in de standaard nen 7510.[48]
De Code voor Informatiebeveiliging en nen 7510 zijn beveiligingsstandaarden die het hele terrein van de informatiebeveiliging binnen een organisatie afdekken. Het zijn algemene, technologieneutrale

[45] Deze standaard is verkrijgbaar bij NEN (http://www.nen.nl/).
[46] Artikel 3 sub b Instellingsbesluit College en Forum Standaardisatie 2012, Stcrt, 2011, 23581.
[47] Het Forum Standaardisatie adviseert op basis van onderzoek het College Standaardisatie over de digitale uitwisseling van informatie tussen overheden onderling en tussen overheid, bedrijven en burgers. Het College doet vervolgens aanbevelingen aan verschillende ministers over beleid op dit gebied en beheert de lijst met aanbevolen en verplichte open standaarden die voor de publieke sector van toepassing zijn. College en Forum Standaardisatie (http://www.forumstandaardisatie.nl/).
[48] NEN, *Steunpunt NEN 7510* (http://www.nen7510.org).

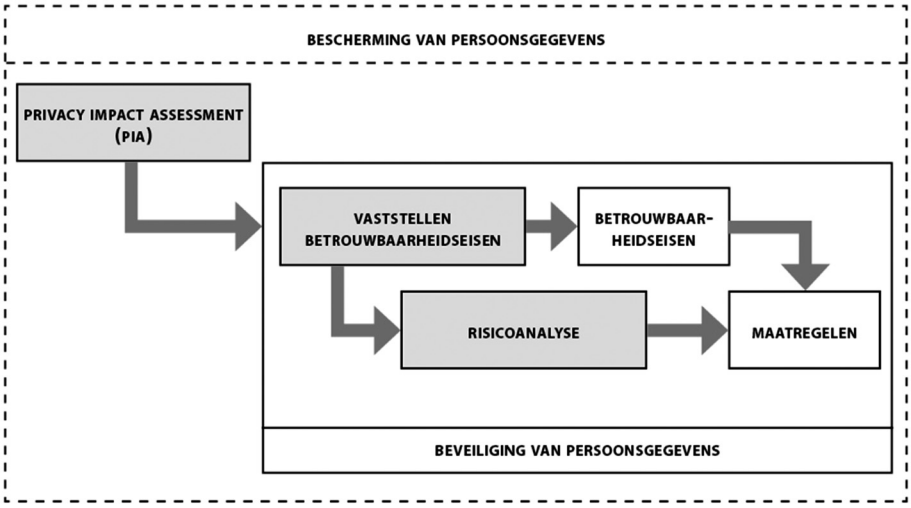
standaarden, wat betekent dat ze niet ingaan op de maatregelen die moeten worden getroffen bij een specifiek type verwerking of bij het gebruik van een specifieke technologie.

Er zijn ook beveiligingsstandaarden die dit wel doen. Voorbeelden zijn de Data Security Standard van de Payment Card Industry voor de veilige afhandeling van creditcardbetalingen[49] en de standaarden voor de beveiliging van *cloud computing* van het Amerikaanse National Institute of Standards and Technology.[50] Voor de beveiliging van webapplicaties zijn er de ict-beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum (ncsc) van het ministerie van Veiligheid en Justitie[51] en voor de beveiliging van mobiele apparaten zijn er de beveiligingsrichtlijnen voor mobiele apparaten van het ncsc.[52] Over het algemeen wordt een optimale beveiliging bereikt door de informatiebeveiliging binnen de organisatie in te richten op basis van een algemene beveiligingsstandaard zoals de Code voor Informatiebeveiliging en bijvoorbeeld bij de ontwikkeling en het beheer van webapplicaties uit te gaan van de ict-beveiligingsrichtlijnen voor webapplicaties van het ncsc.

3 BEVEILIGING IN DE PRAKTIJK

Dit hoofdstuk geeft per onderdeel van de plan-do-check-act-cyclus weer hoe het CBP de beveiliging van persoonsgegevens beoordeelt. Het hoofdstuk beschrijft de beveiliging van persoonsgegevens in algemene zin, waarbij wordt aangesloten op standaarden, methoden en maatregelen die in het vakgebied informatiebeveiliging gebruikelijk zijn. In specifieke situaties kunnen organisaties ook met andere standaarden, methoden en maatregelen het vereiste beveiligingsniveau bereiken. Bij onderzoeken en beoordelingen van de beveiliging van persoonsgegevens is het onderstaande voor het cbp evenwel het uitgangspunt.

Artikel 13 Wbp vereist bij de beveiliging van persoonsgegevens een risicogerichte benadering. Het artikel vraagt om "passende technische en organisatorische maatregelen" die "rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau [garanderen] gelet op de risico"s die de verwerking en de aard van de te beschermen gegevens met zich meebrengen". Deze risicogerichte benadering valt in de praktijk uiteen in een aantal onderdelen, die worden weergegeven in onderstaand schema. In het vervolg van deze paragraaf worden deze onderdelen nader toegelicht.



Het uitvoeren van een privacy impact assessment (pia) helpt de verantwoordelijke om de risico"s te beoordelen die een verwerking van persoonsgegevens met zich meebrengt voor de rechten en vrijheden van de betrokkenen en om maatregelen te treffen die deze risico"s beperken.[53] Een pia wordt als regel uitgevoerd in het eerste ontwerpstadium van een verwerking. De uitkomsten van de

[49] PCI Security Standards Council, *Data security standards overview* (https://www.pcisecuritystandards.org/security_standards/index.php).
[50] NIST, *Cloud computing program* (http://www.nist.gov/itl/cloud/index.cfm).
[51] NCSC, *ICT-beveiligingsrichtlijnen voor webapplicaties* (https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html).
[52] NCSC, *Beveiligingsrichtlijnen voor mobiele apparaten* (https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/beveiligingsrichtlijnen-voor-mobiele-apparaten.html).
[53] In Europese regelgeving wordt voor de PIA de term 'privacyeffectbeoordeling' gebruikt.

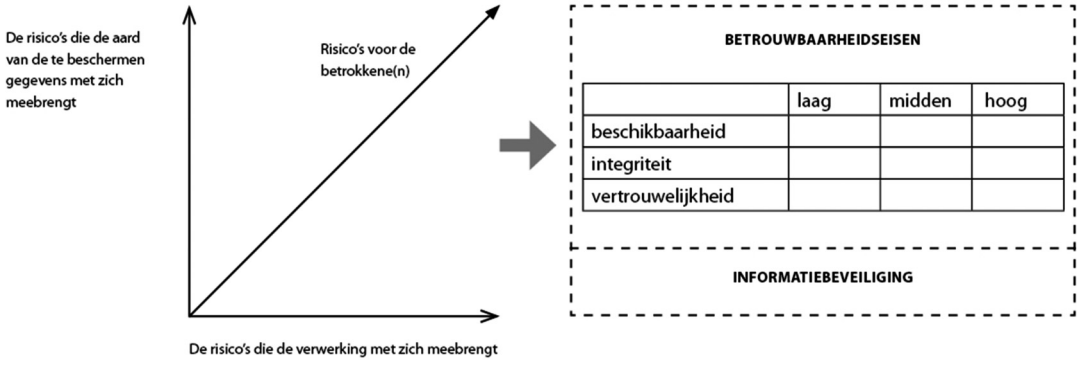
pia kunnen van invloed zijn op de beveiliging van de persoonsgegevens die worden verwerkt, maar kunnen bijvoorbeeld ook leiden tot de keuze om minder persoonsgegevens te verzamelen dan in eerste instantie was voorzien of tot het uitbreiden van de mogelijkheden voor de betrokkenen om zeggenschap uit te oefenen over het gebruik van hun gegevens. De pia valt buiten de reikwijdte van artikel 13 Wbp en van deze richtsnoeren. Wel geeft het uitvoeren van een pia een totaalbeeld van de risico"s voor de betrokkenen en helpt het de verantwoordelijke om beveiligingsmaatregelen te treffen als onderdeel van een samenhangend geheel aan maatregelen waarmee hij de risico"s voor de betrokkenen afdekt en voldoet aan de Wbp.[54]

In het vakgebied informatiebeveiliging vormen de betrouwbaarheidseisen – de eisen aan beschikbaarheid, integriteit en vertrouwelijkheid – het uitgangspunt voor de te treffen beveiligingsmaatregelen.[55] Bij het verwerken van persoonsgegevens dienen de betrouwbaarheidseisen niet uitsluitend te worden vastgesteld vanuit het belang van de verantwoordelijke, maar met name ook vanuit het belang van de betrokkenen. Er is sprake van een "passend beveiligingsniveau gelet op de risico"s die de verwerking en de aard van de te beschermen gegevens met zich meebrengen". Het vaststellen van de betrouwbaarheidseisen vanuit het belang van de betrokkenen wordt nader beschreven in paragraaf 3.1 van deze richtsnoeren.

In het vakgebied informatiebeveiliging is het gangbaar dat de verantwoordelijke beveiligingsmaatregelen treft op basis van een risicoanalyse, waarbij hij de dreigingen inventariseert die kunnen leiden tot een beveiligingsincident, de gevolgen die het beveiligingsincident kan hebben en de kans dat deze gevolgen zich voordoen. De verantwoordelijke kiest de maatregelen zodanig dat wordt voldaan aan de vastgestelde betrouwbaarheidseisen.[56] De risicoanalyse is een belangrijke randvoorwaarde voor "[maatregelen die], rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau [garanderen]".[57] Paragraaf 3.2 van deze richtsnoeren gaat hier nader op in.

3.1 Betrouwbaarheidseisen

De verantwoordelijke stelt vast aan welke eisen betreffende beschikbaarheid, integriteit en vertrouwelijkheid het informatiesysteem moet voldoen. Daarbij draagt hij er zorg voor dat er sprake is van een "passend beveiligingsniveau gelet op de risico"s die de verwerking en de aard van de te beschermen gegevens met zich meebrengen."[58]



Het bovenstaande betekent dat de verantwoordelijke een vertaalslag moet maken van de risico"s voor de betrokkene(n) naar de betrouwbaarheidseisen zoals het vakgebied informatiebeveiliging die kent. Deze vertaalslag is weergegeven in bovenstaand schema. Voor deze vertaalslag zijn vooral de gevolgen relevant die betrokkenen kunnen ondervinden van verlies of onrechtmatige verwerking van hun persoonsgegevens. Deze gevolgen kunnen, afhankelijk van de aard van de verwerking en van de verwerkte persoonsgegevens, onder meer bestaan uit stigmatisering of uitsluiting, schade aan de gezondheid of blootstelling aan (identiteits)fraude.

Voor het vaststellen van de betrouwbaarheidseisen zijn, vanuit de beveiliging van persoonsgegevens en het belang van de betrokkenen bezien, de risico"s voor één, individuele betrokkene maatgevend.

---

[54] De PIA wordt ook genoemd in het regeerakkoord VVD – PvdA, Bruggen slaan, 29 oktober 2012: "Bij de bouw van systemen en het aanleggen van databestanden is bescherming van persoonsgegevens uitgangspunt. Daar hoort een zogenaamd privacy impact assessment (PIA) standaard bij."
[55] Zie paragraaf 2.2 van deze richtsnoeren.
[56] Zie paragraaf 2.4 van deze richtsnoeren.
[57] Artikel 13 Wbp.
[58] Artikel 13 Wbp.

De schade die betrokkenen ondervinden van verlies of onrechtmatige verwerking van hun persoonsgegevens wordt bepaald door de aard van de gegevens en de aard van de verwerking en niet door het aantal anderen van wie de persoonsgegevens eveneens verloren zijn gegaan of onrechtmatig zijn verwerkt.

Voor de genoemde vertaalslag zijn geen algemene regels te geven. Bij verwerkingen met een hoog risico voor de betrokkene(n) is over het algemeen een hoge mate van vertrouwelijkheid vereist. Afhankelijk van de aard van de verwerking geldt hetzelfde voor de integriteit en voor de beveiliging van de persoonsgegevens tegen verlies.

De rest van deze paragraaf gaat nader in op de risico"s die de verwerking en de aard van de te beschermen gegevens met zich meebrengen.
Er is sprake van "een passend beveiligingsniveau gelet op de risico"s die [...] de aard van de te beschermen gegevens met zich meebreng[t]".[59]

De stand van de techniek, ontwikkelingen in de maatschappij en andere factoren kunnen van invloed zijn op de gevolgen die verlies of onrechtmatige verwerking van persoonsgegevens met zich mee kunnen brengen voor de betrokkenen. Onderstaande opsomming van categorieën van persoonsgegevens waar deze gevolgen ernstig kunnen zijn, is daarom niet uitputtend:

- *Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp*
  Het gaat daarbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
- *Gegevens over de financiële of economische situatie van de betrokkene*
  Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden.
- *(Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene*
  Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
- *Gegevens die betrekking hebben op mensen uit kwetsbare groepen*
  Het gaat hier bijvoorbeeld om mensen die te maken hebben met stalking of die in een blijf-van-mijn-lijfhuis verblijven, om klokkenluiders of om informanten van de politie of het Openbaar Ministerie.
- *Gebruikersnamen, wachtwoorden en andere inloggegevens*
  De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.
- *Gegevens die kunnen worden misbruikt voor (identiteits)fraude*

Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het burgerservicenummer (bsn).

Praktijkvoorbeeld: Het e-mailadres als bijzonder persoonsgegeven

Het onderstaande voorbeeld illustreert dat een persoonsgegeven dat op zichzelf niet in de categorie van bijzondere persoonsgegevens valt (het e-mailadres) alsnog een bijzonder persoonsgegeven kan worden door de context waarbinnen het wordt gebruikt.

Een organisatie voor jongeren met belangstelling voor sadomasochisme (sm) organiseert een feest en verstuurt per e-mail een bevestiging van deelname aan iedereen die zich voor dit feest heeft aangemeld. Bij de verzending van de mailing maakt de organisatie een fout, waardoor alle e-mailadressen zichtbaar zijn voor alle 65 ontvangers van de e-mail.
Een e-mailadres is een persoonsgegeven en kan, bijvoorbeeld als het de voor- en achternaam van de betrokkene bevat, de betrokkene direct identificeren. Normaal gesproken is een e-mailadres geen gevoelig gegeven maar in dit geval ontstaat er door de context, deelname aan een sm-feest, een relatie met het seksuele leven van de betrokkene en wordt het gegeven alsnog gevoelig. De verantwoordelijke moet in zo"n geval extra beveiligingsmaatregelen treffen om het uitlekken van de e-mailadressen te voorkomen.

Er is sprake van "een passend beveiligingsniveau gelet op de risico"s die de verwerking [...] met zich meebreng[t]".[60]

[59] Artikel 13 Wbp.
[60] Artikel 13 Wbp.

Behalve de aard van de verwerkte gegevens, kan ook de verwerking zelf risico"s met zich meebrengen voor de betrokkenen. Factoren die een rol spelen zijn onder meer:

- *Hoeveelheid verwerkte persoonsgegevens per persoon*
  Naarmate er per persoon meer persoonsgegevens worden verwerkt, kan verlies of onrechtmatige verwerking leiden tot een grotere inbreuk op de persoonlijke levenssfeer. Bijvoorbeeld: het uitlekken van een compleet medisch dossier leidt over het algemeen tot een grotere inbreuk dan het uitlekken van een herhaalrecept.
- *Doel of doelen waarvoor de persoonsgegevens worden verwerkt*
  Naarmate de beslissingen die op basis van de verwerkte persoonsgegevens worden genomen ingrijpender zijn, is ook de impact van verlies of onrechtmatige verwerking groter. Bijvoorbeeld: als een organisatie financiële gegevens gebruikt om iemands kredietwaardigheid te bepalen zijn de gevolgen ingrijpender dan bij gebruik van dezelfde gegevens voor marketingdoeleinden.

Praktijkvoorbeeld: Beveiliging van via internet toegankelijke bijzondere persoonsgegevens

Onderstaand voorbeeld illustreert hoe de combinatie van de aard van de verwerkte gegevens (bijzondere persoonsgegevens) en de risico"s die de verwerking met zich meebrengt (grote hoeveelheid gegevens per persoon) leidt tot zwaardere eisen aan de beveiliging en, in combinatie met de aanwezige dreigingen, tot aanscherping van de beveiligingsmaatregelen.

Beveiligingsonderzoekers komen erachter dat een webapplicatie die toegang geeft tot elektronische dossiers met persoonsgegevens beveiligingslekken bevat, waardoor onbevoegden toegang kunnen krijgen tot de achterliggende database. De applicatie wordt gebruikt door een groot aantal organisaties. In de applicatie worden bijzondere persoonsgegevens (medische gegevens) en het BSN verwerkt en de hoeveelheid gegevens die per persoon wordt verwerkt is in sommige gevallen aanzienlijk. Onrechtmatige toegang tot de dossiers kan voor de betrokkenen dus grote schade met zich meebrengen. Daarbij gaat het om een webapplicatie, waarbij altijd rekening moet worden gehouden met de mogelijkheid dat een hacker onrechtmatig toegang krijgt tot de verwerkte persoonsgegevens.
De leverancier van de applicatie besluit daarom om niet alleen de beveiligingslekken te dichten, maar ook de beveiliging van de toegang tot de dossiers met persoonsgegevens aan te scherpen door gebruik te maken van zogeheten tweefactorauthenticatie. Gebruikers kunnen in het vervolg alleen nog maar toegang krijgen tot de applicatie als ze beschikken over een combinatie van een wachtwoord en een fysiek herkenningsmiddel (token). Door het gebruik van tweefactorauthenticatie wordt voorkomen dat een hacker door het wachtwoord te achterhalen zich toegang verschaft tot de verwerkte persoonsgegevens.

Bepaalde verwerkingen brengen door de combinatie van de aard van de verwerkte gegevens, de hoeveelheid gegevens die per persoon wordt verwerkt en de doelen waarvoor de persoonsgegevens worden verwerkt dusdanige risico"s met zich mee dat het hoogste beveiligingsniveau is vereist. Verwerkingen in deze categorie zijn onder meer verwerkingen bij opsporingsdiensten met bijzondere bevoegdheden of verwerkingen waarbij de belangen van een grote groep betrokkenen zeer ernstig kunnen worden geschaad indien de verwerkingen onzorgvuldig of onbevoegd geschieden, zoals bij dna-databanken. Daarnaast vallen ook verwerkingen waarop een bijzondere geheimhoudingsplicht van toepassing is binnen deze categorie. Deze geheimhoudingsplicht kan door de overheid zowel wettelijk als anderszins formeel zijn geregeld of door een private organisatie zijn ingevoerd voor haar medewerkers.
Bij dergelijke verwerkingen wordt er al in het vroegste ontwerpstadium rekening gehouden met het vereiste beveiligingsniveau (security by design) en het vereiste niveau van gegevensbescherming (privacy by design). Privacy enhancing technologies (pet) zijn bij dergelijke verwerkingen onmisbaar. Bij de keuze van de beveiligingsmaatregelen is het vereiste beveiligingsniveau leidend. Indien het realiseren van het vereiste beveiligingsniveau tegen acceptabele kosten niet mogelijk is, wordt van verwerking afgezien.

3.2 Maatregelen

Na het vaststellen van de betrouwbaarheidseisen treft de verantwoordelijke passende beveiligingsmaatregelen die waarborgen dat aan de betrouwbaarheidseisen wordt voldaan.

"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 van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau."[61]

[61] Artikel 13 Wbp.

De maatregelen zijn gebaseerd op een risicoanalyse en dekken de risico"s zodanig af dat aan de betrouwbaarheidseisen wordt voldaan.[62] Naarmate de vereiste betrouwbaarheid c.q. het vereiste beveiligingsniveau hoger is, treft de verantwoordelijke meer en zwaardere beveiligingsmaatregelen om de aanwezige risico"s af te dekken en het vereiste beveiligingsniveau daadwerkelijk te garanderen.

Praktijkvoorbeeld: Risicoanalyse door ziekenhuizen

Onderstaand voorbeeld is ontleend aan de toezichtpraktijk van het CBP
Het geeft onder meer weer welke aandachtspunten het CBP in het betreffende onderzoek hanteerde bij de beoordeling van de uitgevoerde risico-analyses.

Gezamenlijk met de Inspectie voor de Gezondheidszorg (IGZ) voert het CBP in 2007 een onderzoek uit naar de mate waarin de normen voor de informatiebeveiliging worden nageleefd door twintig ziekenhuizen.
Bij vijf van de onderzochte ziekenhuizen concluderen IGZ en CBP dat er geen sprake is van een passend beveiligingsniveau zoals bedoeld in artikel 13 Wbp. Na nader onderzoek in 2008 legt het CBP in 2009 aan vier van de ziekenhuizen een last onder dwangsom op, waarbij het CBP de ziekenhuizen onder meer sommeert om een risicoanalyse informatiebeveiliging uit te voeren en daarvan een rapportage op te stellen.
Als toelichting op deze maatregelen verwijst het CBP naar de NEN 7510, waarin de Code voor Informatiebe-veiliging voor de zorgsector nader is uitgewerkt en die als een gezaghebbende en sectorale uitwerking van artikel 13 Wbp wordt beschouwd.

Het CBP geeft daarbij het volgende aan:
"Een risicoanalyse vormt de basis voor het informatiebeveiligingsbeleid van een organisatie. Zonder risicoanalyse is het niet mogelijk om een adequaat informatiebeveiligingsbeleid te formuleren: pas na een risicoanalyse kunnen de prioritaire maatregelen voor informatiebeveiliging worden bepaald.
De definitie van een risicoanalyse in NEN 7510 – 'beoordeling van de bedreigingen voor, effecten op en kwetsbaarheid van informatiesystemen en gegevens en de waarschijnlijkheid van het optreden van deze bedreigingen' is gangbaar binnen het vakgebied informatiebeveiliging en geeft een organisatie – binnen de grenzen van de definitie – de vrijheid zelf een risicoanalysemethode te kiezen. Zodra echter elementen uit de definitie ontbreken is de risicoanalyse ontoereikend en wordt gezien het boven-staande niet voldaan aan de norm van artikel 13 Wbp."

Het cbp constateert dat twee van de vier ziekenhuizen in eerste instantie een risicoanalyse hebben uitgevoerd die niet voldoet aan de last. In de risicoanalyse van één ziekenhuis ontbreekt een inventarisatie van de (reële) bedreigingen, is er geen zicht op de kwetsbaarheid van de informatiesys-temen en is er onvoldoende zicht op de beveiligingsmaatregelen die al zijn geïmplementeerd, waardoor er niet kan worden afgebakend welke maatregelen er uiteindelijk nog moeten worden getroffen. Het tweede ziekenhuis heeft aan de hand van een checklist in kaart gebracht hoe informatie-beveiliging volgens NEN7510 in de dagelijkse praktijk wordt toegepast, wat geen of hooguit zeer beperkt inzicht geeft in de concrete ICT-risico"s die het ziekenhuis loopt.

Beide ziekenhuizen vullen de risicoanalyse aan, zodat zij uiteindelijk alsnog aan de last voldoen.

De risicoanalyse geeft aan welke risico"s moeten worden afgedekt; beveiligingsstandaarden geven houvast bij het daadwerkelijk treffen van passende maatregelen om de risico"s af te dekken. Welke beveiligingsstandaarden voor een bepaalde verwerking relevant zijn en welke beveiligingsmaatrege-len op grond van deze beveiligingsstandaarden moeten worden getroffen, moet van geval tot geval worden bepaald.

Bij het onderzoeken en beoordelen van de beveiliging van persoonsgegevens hanteert het CBP als uitgangspunt een aantal beveiligingsmaatregelen die binnen het vakgebied informatiebeveiliging gebruikelijk zijn en die in veel situaties in een of andere vorm noodzakelijk zijn. Het gaat om de volgende maatregelen:
- *Beleidsdocument voor informatiebeveiliging*[63]
  Het beleidsdocument gaat expliciet in op de maatregelen die de verantwoordelijke treft om de verwerkte persoonsgegevens te beveiligen. Het document is goedgekeurd op bestuurlijk c.q. leidinggevend niveau en kenbaar gemaakt aan alle werknemers en relevante externe partijen.
- *Toewijzen van verantwoordelijkheden voor informatiebeveiliging*[64]

[62] Zie paragraaf 2.4 van deze richtsnoeren.
[63] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 5.1.1.
[64] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 6.1.3.

Alle verantwoordelijkheden, zowel op sturend als op uitvoerend niveau, zijn duidelijk gedefinieerd en belegd.

- *Beveiligingsbewustzijn*[65]
  Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers krijgen geschikte training en regelmatige bijscholing over het informatiebeveiligingsbeleid en de informatiebeveiligingsprocedures van de organisatie, voor zover relevant voor hun functie. Binnen de training en bijscholing wordt expliciet aandacht besteed aan de omgang met (bijzondere of anderszins gevoelige) persoonsgegevens.
- *Fysieke beveiliging en beveiliging van apparatuur*[66]
  IT-voorzieningen en apparatuur zijn fysiek beschermd tegen toegang door onbevoegden en tegen schade en storingen. De geboden bescherming is in overeenstemming met de vastgestelde risico"s.
- *Toegangsbeveiliging*[67]
  Er zijn procedures om bevoegde gebruikers toegang te geven tot de informatiesystemen en -diensten die ze voor de uitvoering van hun taken nodig hebben en om onbevoegde toegang tot informatiesystemen te voorkomen. De procedures omvatten alle fasen in de levenscyclus van de gebruikerstoegang, van de eerste registratie van nieuwe gebruikers tot de uiteindelijke afmelding van gebruikers die niet langer toegang tot informatiesystemen en -diensten nodig hebben. Waar van toepassing wordt bijzondere aandacht besteed aan het beheren van toegangsrechten van gebruikers met extra ruime bevoegdheden, zoals systeembeheerders.
- *Logging en controle*[68]
  Activiteiten die gebruikers uitvoeren met persoonsgegevens worden vastgelegd in logbestanden. Hetzelfde geldt voor andere relevante gebeurtenissen, zoals pogingen om ongeautoriseerd toegang te krijgen tot persoonsgegevens en verstoringen die kunnen leiden tot verminking of verlies van persoonsgegevens. De logbestanden worden periodiek gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van de persoonsgegevens en waar nodig wordt actie ondernomen.
  De verantwoordelijke moet er rekening mee houden dat er, als de gegevens in de logbestanden tot personen herleidbaar zijn, sprake is van een verwerking van persoonsgegevens in de zin van de Wbp waarop de verplichtingen uit deze wet van toepassing zijn. In dat geval kan er ook sprake zijn van een personeelsvolgsysteem in de zin van artikel 27 lid 1 van de Wet op de ondernemingsraden (WOR), waarvoor instemming van de ondernemingsraad is vereist.
- *Correcte verwerking in toepassingssystemen*[69]
  In alle toepassingssystemen, inclusief toepassingen die door gebruikers zelf zijn ontwikkeld, zijn beveiligingsmaatregelen ingebouwd. Tot deze beveiligingsmaatregelen behoort de controle dat de invoer, de interne verwerking en de uitvoer aan vooraf gestelde eisen voldoen (validatie). Voor systemen waarin gevoelige persoonsgegevens worden verwerkt of die invloed hebben op de verwerking van gevoelige persoonsgegevens, kunnen aanvullende beveiligingsmaatregelen nodig zijn.
- *Beheer van technische kwetsbaarheden*[70]
  Software, zoals browsers, virusscanners en operating systems, wordt up-to-date gehouden. Ook installeert de verantwoordelijke tijdig oplossingen die de leverancier uitbrengt voor beveiligingslekken in deze software. Meer in het algemeen verkrijgt de verantwoordelijke tijdig informatie over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden wordt geëvalueerd en de verantwoordelijke treft geschikte maatregelen getroffen voor de behandeling van de risico"s die daarmee samenhangen.
- *Incidentenbeheer*[71]
  Er zijn procedures voor het tijdig en doeltreffend behandelen van informatiebeveiligingsincidenten en zwakke plekken in de beveiliging, zodra ze zijn gerapporteerd. Het beoordelen van de risico"s voor de betrokkenen en het effectief informeren van de betrokkenen en, waar van toepassing, de toezichthouder is in deze procedures opgenomen. De lessen getrokken uit de afgehandelde incidenten worden gebruikt om de beveiliging waar mogelijk structureel te verbeteren. Als een vervolgprocedure na een informatiebeveiligingsincident juridische maatregelen omvat (civiel- of strafrechtelijk), wordt het bewijsmateriaal verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.
- *Afhandeling van datalekken en beveiligingsincidenten*[72]

[65] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 8.2.2.
[66] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 9.1 en 9.2.
[67] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 11.2.
[68] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 10.10.
[69] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 12.2.
[70] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 12.6.
[71] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 13.2.
[72] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 13.1.2.

De verantwoordelijke meldt datalekken die onder een wettelijke meldplicht vallen bij de betreffende toezichthouder.[73] Als hij daartoe wettelijk verplicht is, of als er anderszins aanleiding voor is, informeert hij ook de betrokkenen over het beveiligingsincident of het datalek.

- *Continuïteitsbeheer*[74]
  Door natuurrampen, ongevallen, uitval van apparatuur of opzettelijk handelen kunnen persoonsgegevens verloren gaan. Door in de organisatie continuïteitsbeheer in te richten worden de gevolgen tot een aanvaardbaar niveau beperkt, waarbij gebruik wordt gemaakt van een combinatie van preventieve maatregelen en herstelmaatregelen.

Er is pas sprake van een passend beveiligingsniveau als de gekozen maatregelen onderdeel zijn van de dagelijkse praktijk van de organisatie. De eerste stap is documentatie: de relevante beveiligingsmaatregelen zijn gespecificeerd en geïntegreerd in functionele en technische beschrijvingen van ict-systemen, in gebruikershandleidingen, werkinstructies, contracten, dienstenniveauovereenkomsten en andere relevante documenten. De tweede stap is daadwerkelijke implementatie van de gekozen maatregelen.

"Een ieder die handelt onder het gezag van de verantwoordelijke of van de bewerker, alsmede de bewerker zelf, voor zover deze toegang hebben tot persoonsgegevens, verwerkt deze slechts in opdracht van de verantwoordelijke, behoudens afwijkende wettelijke verplichtingen."[75]

De hierboven genoemde maatregelen 'beveiligingsbewustzijn', 'toegangsbeveiliging' en 'logging en controle' zijn er mede op gericht om ongeoorloofde omgang met persoonsgegevens binnen de organisatie tegen te gaan.

"De personen, bedoeld in het eerste lid, voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit."[76]

Bij het onderzoeken en beoordelen van de beveiliging van persoonsgegevens hanteert het CBP, waar het gaat om de geheimhouding van de verwerkte persoonsgegevens, als uitgangspunt een aantal maatregelen die in het vakgebied informatiebeveiliging gangbaar zijn. Deze maatregelen zijn:

- *Gegevensbescherming en geheimhouding van persoonsgegevens*[77]
  De organisatie heeft beleid ontwikkeld voor de bescherming en voor de geheimhouding van persoonsgegevens. Dit beleid is vastgelegd en geïmplementeerd en de organisatie communiceert dit naar alle personen die betrokken zijn bij het verwerken van persoonsgegevens. In het beleid is opgenomen dat persoonsgegevens uitsluitend worden verwerkt in opdracht van de verantwoordelijke.
- *Geheimhoudingsovereenkomsten*[78]
  De verplichting tot geheimhouding van persoonsgegevens is vastgelegd in geheimhoudingsovereenkomsten.

Praktijkvoorbeeld: Onrechtmatige inzage in een medisch dossier

Onderstaand voorbeeld illustreert wat wordt bedoeld met ongeoorloofde omgang met persoonsgegevens binnen de organisatie.

In 2007 doet het cbp samen met de Inspectie voor de Gezondheidszorg (IGZ) onderzoek naar de informatiebeveiliging bij een aantal ziekenhuizen. Uit het onderzoek blijkt dat de directie van een van de onderzochte ziekenhuizen wel heel persoonlijk is geconfronteerd met het belang van informatiebeveiliging. Tijdens een opname van de voorzitter van de Raad van Bestuur in zijn eigen ziekenhuis

---

[73] Bij het verschijnen van deze richtsnoeren is de situatie rond de meldplicht voor datalekken als volgt:
• Er is een meldplicht van toepassing voor aanbieders van openbare telecommunicatienetwerken en -diensten (http://www.meldplichttelecomwet.nl/inbreuken.html).
• In december 2011 is een voorstel tot aanpassing van de Wbp gepresenteerd. Het voorstel bevat een verplichting om beveiligingsincidenten te melden bij het CBP waarvan redelijkerwijs kan worden aangenomen dat die leiden tot een aanmerkelijk risico op verlies of onrechtmatige verwerking en waaraan nadelige gevolgen voor de persoonsgegevens en de persoonlijke levenssfeer van de betrokkene zijn verbonden (http://www.internetconsultatie.nl/camerabeelden).
• De Europese Commissie heeft een conceptverordening gepresenteerd die de huidige richtlijn 95/46/EG, waarop de Wbp gebaseerd is, moet gaan vervangen. In de conceptverordening is een verplichting opgenomen om datalekken te melden bij de toezichthoudende autoriteit (http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm).

[74] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 14.

[75] Artikel 12 lid 1 Wbp.

[76] Artikel 12 lid 2 Wbp.

[77] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 15.1.4.

[78] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 6.1.5.

hebben namelijk verschillende medewerkers die hem niet behandelden zich toegang verschaft tot zijn elektronisch medisch dossier.[79]

"De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen."[80]

Bij het onderzoeken en beoordelen van de naleving van de wettelijke verplichting tot het toepassen van pet hanteert het CBP als uitgangspunt een aantal gangbare pet-maatregelen. Deze maatregelen zijn:

- *Encryptie (versleuteling) en hashing*[81]
  De verantwoordelijke maakt gebruik van cryptografische bewerkingen om de persoonsgegevens die hij verwerkt te beveiligen. Hij past encryptie (versleuteling) toe bij verzending van persoonsgegevens via het internet, bij de opslag van persoonsgegevens op draagbare apparatuur en op verwijderbare media zoals usb-sticks en in andere situaties waar persoonsgegevens kwetsbaar zijn voor toegang door onbevoegden (bijvoorbeeld persoonsgegevens die via het world wide web kunnen worden benaderd). Bij de opslag en verwerking van wachtwoorden maakt hij gebruik van hashing. Bij het toepassen van cryptografische technieken past hij alle gangbare voorzorgsmaatregelen toe, zoals goed ingericht sleutelbeheer en het gebruik van sleutellengten en versleutelingstechnieken die in overeenstemming zijn met de actuele stand van de techniek.
- *Omgang met e-waste (afgedankte apparatuur en opslagmedia)*
  Alle apparatuur die opslagmedia bevat, zoals laptops of smartphones, wordt ontdaan van de nog eventueel aanwezige persoonsgegevens alvorens het apparaat te verwijderen of hergebruiken. Opslagmedia met gevoelige persoonsgegevens worden fysiek vernietigd of de persoonsgegevens worden vernietigd, verwijderd of overschreven met technieken die het onmogelijk maken om de oorspronkelijke persoonsgegevens terug te halen.[82] Hetzelfde geldt voor verwijderbare media zoals usb-sticks.[83]

Nader bekeken: Encryptie, hashing, pseudonimisering en anonimisering

Onderstaand worden de cryptografische bewerkingen encryptie en hashing toegelicht. Verder wordt aangegeven dat toepassing van deze cryptografische bewerkingen op zichzelf leidt tot pseudonimisering (het vervangen van een identificerend gegeven door een ander identificerend gegeven) en niet tot anonimisering.

Encryptie (versleuteling) en hashing (het omzetten van gegevens in een unieke code) zijn cryptografische bewerkingen die worden toegepast op gegevens met onder meer als doel om deze onbruikbaar te maken voor onbevoegden.
Kenmerkend voor encryptie is dat deze bewerking omkeerbaar is: door gebruik van de juiste sleutel kan de oorspronkelijke informatie worden verkregen (decryptie). Encryptie wordt onder meer gebruikt om gegevens te beveiligen bij verzending van gegevens via het internet, bij de opslag van gegevens op draagbare apparatuur en op verwijderbare media zoals USB-sticks en in andere situaties waar gegevens kwetsbaar zijn voor toegang door onbevoegden (bijvoorbeeld gegevens die via het world wide web kunnen worden benaderd).
Hashing is een bewerking die van informatie, ongeacht de lengte, een unieke hashcode maakt die altijd even lang is (de lengte is afhankelijk van de gebruikte hashingmethode). Hashing wordt onder meer gebruikt bij de opslag en verwerking van wachtwoorden: op het moment dat de gebruiker een (nieuw) wachtwoord kiest, wordt de bijbehorende hashcode opgeslagen. Wanneer de gebruiker vervolgens inlogt, wordt de hashcode van het ingevoerde wachtwoord vergeleken met de opgeslagen hashcode en krijgt de gebruiker toegang tot het informatiesysteem als de codes overeenkomen.

Cryptografische bewerkingen zijn in principe te 'kraken', wat inhoudt dat onbevoegden toegang kunnen krijgen tot de oorspronkelijke gegevens. Kraken wordt tegengegaan door het gebruik van (combinaties van) de nieuwste cryptografische technieken en door toepassing van zogenoemde salts (extra informatie die bij hashing wordt toegevoegd aan het oorspronkelijke gegeven om het kraken van de hashcode te bemoeilijken). Dit terrein ontwikkelt zich voortdurend en het is zeer goed mogelijk dat een cryptografische bewerking die in de huidige situatie veilig genoeg is dat over een aantal jaren niet meer is. Bij gebruik van cryptografische bewerkingen wordt daarom periodiek beoordeeld of nog

---

[79] Inspectie voor de Gezondheidszorg (IGZ) en CBP, *Informatiebeveiliging in ziekenhuizen voldoet niet aan de norm, Rapportage van een onderzoek in 2007 door het College bescherming persoonsgegevens en de Inspectie voor de Gezondheidszorg naar de informatiebeveiliging in 20 ziekenhuizen,* Den Haag, november 2008, p. 26.
(http://www.cbpweb.nl/downloads_rapporten/rap_2008_informatiebeveiliging_ziekenhuizen.pdf)
[80] Artikel 13 Wbp.
[81] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 12.3.
[82] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 9.2.6.
[83] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 10.7.2.

steeds wordt voldaan aan de betrouwbaarheidseisen.

Door toepassing van encryptie en hashing kan de mate waarin de verwerkte persoonsgegevens kunnen worden herleid naar "een geïdentificeerde of identificeerbare natuurlijke persoon" worden verminderd. Een voorbeeld is het versleutelen of hashen van klantnummers. Het toepassen van cryptografische bewerkingen op identificerende gegevens leidt op zichzelf tot pseudonimisering (het identificerende gegeven wordt vervangen door een ander identificerend gegeven) en niet tot anonimisering (de gegevens worden omgezet naar "een vorm die identificatie van de betrokkene feitelijk niet langer mogelijk maakt"[84]).

Nog afgezien van de mogelijkheid dat de gebruikte cryptografische bewerkingen gekraakt worden, leidt het toepassen van cryptografische bewerkingen op identificerende gegevens om de volgende redenen tot pseudonimisering en niet tot anonimisering:
- Encryptie is *omkeerbaar*. De verantwoordelijke beschikt over de juiste sleutel en is daarmee in staat om decryptie toe te passen op het versleutelde gegeven en daardoor het oorspronkelijke identificerende gegeven te achterhalen.
- Encryptie en hashing zijn *herhaalbaar*. De verantwoordelijke beschikt over de oorspronkelijke gegevens en kan door deze opnieuw te versleutelen of hashen de bijbehorende versleutelde gegevens of hashcodes achterhalen.

De verantwoordelijke kan maatregelen treffen om bij gebruik van encryptie of hashing de herleidbaarheid van de betreffende persoonsgegevens te beperken, bijvoorbeeld door de cryptografische bewerking uit te laten voeren door een derde die als enige over de juiste sleutel beschikt. Van geval tot geval moet een verantwoordelijke vaststellen of dergelijke maatregelen daadwerkelijk leiden tot anonimisering.

Voor anonimisering zijn niet alleen de direct identificerende gegevens van belang. "Het verwijderen van de direct identificerende kenmerken biedt op zichzelf niet altijd voldoende garantie dat geen sprake meer is van persoonsgegevens. Door middel van spontane herkenning, vergelijking van gegevens en/of koppeling aan gegevens uit andere bron, kan immers desondanks, soms zonder bijzonder inspanning, identificatie tot stand worden gebracht."[85] Verder moet bij anonimisering rekening worden gehouden met de stand van de techniek. "Wat [...] bij een bepaalde stand van de techniek als anoniem, want redelijkerwijs niet op een persoon herleidbaar gegeven, kan worden beschouwd, kan door technische ontwikkelingen alsnog een persoonsgegeven worden gelet op de toegenomen mogelijkheden tot herleiding."[86]

3.3 Controle

De verantwoordelijke stelt vast of de maatregelen daadwerkelijk getroffen zijn en worden nageleefd en of de organisatie door het treffen van deze maatregelen aan de betrouwbaarheidseisen voldoet.

De verantwoordelijke stelt vast of de technische en organisatorische maatregelen in de praktijk worden nageleefd en of deze een passend beveiligingsniveau garanderen. Waar nodig voert hij aanpassingen door.

Bij onderzoek en beoordeling hanteert het CBP als uitgangspunt de volgende controles die in het vakgebied informatiebeveiliging gangbaar zijn:
- *Controle op naleving van de maatregelen binnen de organisatie*[87]
  De verantwoordelijke beoordeelt regelmatig of de beveiligingsmaatregelen binnen de organisatie daadwerkelijk worden nageleefd. Waar dit niet gebeurt, treft de verantwoordelijke corrigerende maatregelen.
- *Controle op technische naleving*[88]
  De verantwoordelijke beoordeelt regelmatig of de beveiligingsmaatregelen binnen de technische systemen daadwerkelijk worden nageleefd.

Verder betrekt het CBP hierbij de inzet van de volgende gangbare middelen voor de controle op uitvoering en naleving van de beveiligingsmaatregelen:
- *Werkplekcontroles*
  Buiten kantooruren laat de verantwoordelijke controleren of er documenten met gevoelige

[84] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 50.
[85] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 48.
[86] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 49.
[87] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 15.2.1.
[88] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 15.2.2.

persoonsgegevens aanwezig zijn op werkplekken, in vergaderruimtes, bij printers of kopieerapparaten of in niet-afgesloten papierbakken. Op deze manier kan de verantwoordelijke vaststellen of de gedragsregels voor de omgang met documenten met gevoelige persoonsgegevens effectief zijn en afdoende bekend zijn gemaakt binnen de organisatie.

- *Social engineering tests*
  In deze tests proberen experts per telefoon of per e-mail om, vaak onder valse voorwendselen, persoonsgegevens 'los te krijgen'. Door dergelijke tests uit te laten voeren kan de verantwoordelijke vaststellen in hoeverre gedragsregels voor het verstrekken van persoonsgegevens daadwerkelijk worden nageleefd.
- *Beoordeling van de beveiligingsmaatregelen in toepassingssystemen*[89]
  De verantwoordelijke laat een code review (een inspectie van de programmacode) uitvoeren om vast te stellen of de beveiligingsmaatregelen die zijn ingebouwd in de toepassingssystemen nog steeds toereikend zijn of dat deze bijvoorbeeld moeten worden aangepast aan de stand van de techniek of aan de nieuwste inzichten in de informatiebeveiliging. Bij toepassingen die worden onderhouden door een externe partij worden daarnaast ook de werkzaamheden van deze derde partij beoordeeld: hoe snel verhelpt deze bijvoorbeeld geconstateerde kwetsbaarheden of beveiligingslekken in het toepassingssysteem?
- *Tests van nieuwe en gewijzigde informatiesystemen*[90]
  De bekendste vorm hiervan is waarschijnlijk de penetratietest, waarin experts proberen om de beveiliging van een informatiesysteem te doorbreken. Over het algemeen gaat hier een aantal andere tests aan vooraf, waarin de experts per informatiesysteem of per subsysteem vaststellen of de gespecificeerde beveiligingsmaatregelen daadwerkelijk zijn getroffen. De functie van de penetratietest is vooral het blootleggen van onvoorziene risico"s of zwakke plekken in de beveiliging.
- *Beveiligingsassessments*
  In dergelijke assessments wordt vastgesteld in hoeverre de gekozen beveiligingsmaatregelen daadwerkelijk zijn geïmplementeerd en worden nageleefd. Bovengenoemde controlemiddelen kunnen hier deel van uitmaken.

Nader bekeken: Papier hier...

Onderstaand wordt ingegaan op de beveiliging van persoonsgegevens die op papier worden verwerkt en wordt aangegeven hoe de controle op naleving past binnen het totaal aan beveiligingsmaatregelen.

De meeste organisaties verwerken persoonsgegevens niet alleen in geautomatiseerde systemen maar ook op papier. Bij dat laatste gaat het niet alleen om papieren dossiers maar bijvoorbeeld ook om documenten uit een elektronisch dossier die worden uitgeprint om ze in een vergadering te bespreken. Als de organisatie hier onvoldoende zorgvuldig mee omgaat, kunnen er ondanks alle overige beveiligingsmaatregelen alsnog persoonsgegevens weglekken.

Preventieve maatregelen bestaan allereerst uit het opstellen en binnen de organisatie bekend maken van gedragsregels. Middelen waarvan de organisatie gebruik kan maken bij een veilige omgang met persoonsgegevens op papier zijn afsluitbare dossierkasten en papierversnipperaars of afsluitbare prullenbakken voor vertrouwelijke stukken, waarvan de inhoud door een gespecialiseerd bedrijf wordt verwijderd en vernietigd. Controle op de naleving van de gedragsregels is noodzakelijk, met name voor organisaties die gevoelige gegevens op papier verwerken. Door werkplekcontroles wordt vastgesteld dat er aan het einde van de werkdag geen documenten met gevoelige persoonsgegevens op werkplekken zijn achtergebleven, dat er geen gevoelige informatie bij printers of kopieerapparaten of in vergaderkamers ligt en dat alle dossierkasten zijn afgesloten. Deze controle is extra belangrijk als de organisatie gebruikmaakt van een locatie die toegankelijk is voor het publiek, zoals een gemeentehuis, of die gedeeld wordt met andere organisaties.

3.4 Evaluatie en aanpassing

In de evaluatie bepaalt de verantwoordelijke onder meer of de vastgestelde betrouwbaarheidseisen nog steeds aansluiten bij de risico"s die de verwerking en de aard van de te verwerken gegevens met zich meebrengen en of door de getroffen maatregelen nog steeds aan de betrouwbaarheidseisen wordt voldaan.

De verantwoordelijke stelt periodiek, of wanneer de omstandigheden daar aanleiding toe geven, vast of de getroffen "technische en organisatorische maatregelen" nog steeds een "passend beveiligings-

[89] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 12.5.5.
[90] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 10.3.2.

niveau [garanderen]".[91] *("Met zich ontwikkelende techniek zal periodiek een nieuwe afweging moeten worden gemaakt.")*[92] *Waar nodig voert hij aanpassingen door.*

Bij grote veranderingen in de organisatie of in de informatiesystemen stelt de verantwoordelijke vast of het bestaande pakket aan beveiligingsmaatregelen nog steeds voldoet aan het vereiste beveiligingsniveau. Voorbeelden van dergelijke veranderingen zijn:

- *Nieuwe locatie*
  De organisatie verhuist van een eigen gebouw, dat met elektronische toegangspasjes was beveiligd, naar werkplekken in een open kantoortuin die wordt gedeeld met medewerkers van een andere organisatie.
- *Nieuwe taken*
  De organisatie krijgt nieuwe taken, waardoor er per betrokkene veel meer persoonsgegevens worden verwerkt.
- *Nieuwe functionaliteit*
  De organisatie besluit om een internetportaal te creëren waarmee betrokkenen inzage kunnen krijgen in de persoonsgegevens die de organisatie van hen verwerkt.
- *Nieuwe werkwijze en technologie*

De organisatie introduceert 'het nieuwe werken', wat onder meer inhoudt dat medewerkers hun eigen apparatuur aan kunnen sluiten op het interne netwerk van de organisatie.

Waar nodig stelt de verantwoordelijke de betrouwbaarheidseisen bij op basis van de nieuwe situatie en/of past hij het pakket beveiligingsmaatregelen aan.

Verder kunnen de stand van de techniek en de kosten van de uitvoering van beveiligingsmaatregelen in de loop van de tijd veranderen. Ook kan de aard van de verwerking of van de verwerkte persoonsgegevens in de loop van de tijd leiden tot nieuwe of andere risico"s voor de betrokkenen, bijvoorbeeld als gevolg van maatschappelijke ontwikkelingen. Om te kunnen blijven spreken van passende maatregelen, of van die maatregelen die in redelijkheid mogen worden verwacht, is het dan ook noodzakelijk om periodiek te bepalen of de vastgestelde betrouwbaarheidseisen nog steeds aansluiten bij de risico"s die de verwerking en de aard van de te beschermen gegevens met zich meebrengen en de beveiligingsmaatregelen waar nodig bij te stellen. Bij dit laatste neemt de verantwoordelijke ook de getrokken lessen uit de opgetreden beveiligingsincidenten mee.

4 BEVEILIGING BIJ VERWERKING DOOR EEN BEWERKER

Veel verantwoordelijken (organisaties die persoonsgegevens verwerken) laten hun persoonsgegevens verwerken door een zogeheten bewerker. Van verwerking door een bewerker is bijvoorbeeld sprake bij gebruik van een extern callcenter voor klantcontacten, bij het verwerken van persoonsgegevens in de cloud of bij externe hosting van een website waarbij persoonsgegevens worden verwerkt.[93, 94, 95] Dit hoofdstuk geeft weer hoe het CBP de beveiliging van persoonsgegevens beoordeelt bij verwerking door een bewerker. Het hoofdstuk moet worden gelezen in samenhang met hoofdstuk 3: hoofdstuk 3 geeft in het algemeen weer hoe het CBP de beveiliging van persoonsgegevens beoordeelt en hoofdstuk 4 bevat de specifieke uitgangspunten voor verwerking door een bewerker.

4.1 Risicoanalyse van verwerking door een bewerker

De verantwoordelijke voert een risicoanalyse uit betreffende de verwerking door een bewerker.

In de risicoanalyse stelt de verantwoordelijke vast of en zo ja, onder welke voorwaarden, de bewerker "voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen" en de verantwoordelijke voldoende in staat is om "toe [te zien] op de naleving van die maatregelen."[96] *Verder stelt hij vast of en zo ja, onder welke*

---

[91] Artikel 13 Wbp.
[92] Kamerstukken I 1999-2000, 25 892, nr. 92c, p. 15.
[93] Het CBP heeft een zienswijze uitgebracht waarin een aantal vragen over cloud computing wordt beantwoord. CBP, *Zienswijze inzake de toepassing van de Wet bescherming persoonsgegevens bij een overeenkomst met betrekking tot cloud computing diensten van een Amerikaanse leverancier*, 7 augustus 2012 (http://www.cbpweb.nl/Pages/med_20120910-zienswijze-cbp-cloudcomputing.aspx).
[94] Het onafhankelijk overlegorgaan van de privacytoezichthouders van de lidstaten van de Europese Unie heeft een advies uitgebracht over de privacyaspecten van cloud computing. Groep Gegevensbescherming Artikel 29 (WP29), *Advies 05/2012 over Cloud Computing*, Goedgekeurd op 1 juli 2012 (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_nl.pdf).
[95] Het NCSC heeft een publicatie uitgebracht over cloud computing en beveiliging. NCSC, *Cloud computing & security*, januari 2012 (https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/whitepaper-cloudcomputing.html).
[96] Artikel 14 lid 1 Wbp.

voorwaarden, er voldoende waarborgen zijn dat de bewerker "de verplichtingen nakomt die op de verantwoordelijke rusten ingevolge artikel 13."[97]

In de risicoanalyse betrekt de verantwoordelijke in ieder geval de gangbaarste dreigingen en kwetsbaarheden die samenhangen met verwerking door een bewerker en de mogelijke gevolgen voor de betrokkenen. Welke dreigingen en kwetsbaarheden in een specifieke situatie daadwerkelijk aanwezig zijn, hangt onder meer af van de aard van de dienstverlening. Het vervolg van deze paragraaf geeft de gangbaarste dreigingen en kwetsbaarheden weer die samenhangen met de verwerking van persoonsgegevens door een bewerker.

Als de bewerker onvoldoende beveiligingsmaatregelen treft, dan kan dat leiden tot verlies of onrechtmatige verwerking van de verwerkte persoonsgegevens. Onder meer zijn hier de volgende kwetsbaarheden te onderkennen:

- *Onvoldoende beveiliging van de verwerkte persoonsgegevens*
  Verwerking door een bewerker betekent dat de verantwoordelijke, behalve de bewerking zelf, ook de beveiliging van de verwerkte persoonsgegevens uit handen geeft. Als de verantwoordelijke bijvoorbeeld gebruikmaakt van de diensten van een hostingprovider, dan zal deze ook een groot deel van de beveiliging van de betreffende website voor zijn rekening nemen.[98] Daarbij gaat het onder meer om maatregelen zoals logging en controle (het vastleggen van belangrijke gebeurtenissen en het controleren op tekenen van onrechtmatige toegang tot de verwerkte gegevens) en het up-to-date houden van de systeemprogrammatuur op de webserver. Dit zijn beveiligingsmaatregelen die de verantwoordelijke niet zelf kan treffen, omdat hij slechts in beperkte mate toegang heeft tot de webserver en in veel gevallen ook de benodigde expertise mist. Als de bewerker hierin tekortschiet, kan dat leiden tot verlies of onrechtmatige verwerking van de verwerkte persoonsgegevens.
- *Onvoldoende beveiliging van de dienstverlening door de bewerker*
  De bewerker biedt in veel gevallen faciliteiten waarmee de verantwoordelijke de persoonsgegevens kan uploaden die door de bewerker moeten worden bewerkt of waarmee de verantwoordelijke de verwerkte persoonsgegevens kan raadplegen of aanpassen. Onvoldoende beveiliging van deze faciliteiten kan leiden tot verlies of onrechtmatige verwerking van de persoonsgegevens.

Praktijkvoorbeeld: Beveiligingsincidenten bij verwerking door een bewerker

Onderstaande voorbeelden illustreren de dreiging van onvoldoende beveiliging van de verwerkte gegevens door de bewerker.

De onderstaande praktijkvoorbeelden kwamen in 2012 in het nieuws:

- Door een beveiligingsfout in een website kan een hacker zich toegang verschaffen tot de server waarop de website zich bevindt. Op de server treft de hacker ruim 150 databases aan die toebehoren aan verschillende organisaties, waaronder een database met 12.000 e-mailadressen die afkomstig zijn uit een marketingactie. De databases zijn allemaal volledig toegankelijk als gevolg van een menselijke fout van de ICT-dienstverlener die de server beheert.
- Een hacker breekt in bij een online verkoper van theaterkaarten. Hij ontdekt op de server een database die zonder wachtwoord te benaderen is, met daarin ruim vierenhalfmiljoen databaseregels die onder meer (deels verouderde) creditcardgegevens bevatten. Hij constateert dat de database zonder wachtwoord toegankelijk is als gevolg van aanpassingen op de server die zijn uitgevoerd bij een eerdere hack. De ICT-dienstverlener die de server beheert, heeft de eerdere hack niet bemerkt.

Naast onvoldoende beveiliging kan onvoldoende transparantie van de kant van de bewerker ertoe leiden dat de verantwoordelijke niet voldoet aan zijn wettelijke verplichtingen. Hierbij zijn onder meer de volgende situaties te onderkennen:

- *Onvoldoende transparantie over de beveiliging*
  De verantwoordelijke moet zorgen dat de bewerker voldoende technische en organisatorische beveiligingsmaatregelen treft en hij moet toezien op de naleving. Als de verantwoordelijke onvoldoende inzicht heeft in het geboden beveiligingsniveau of als hij niet vast kan stellen of de bewerker de overeengekomen beveiligingsmaatregelen daadwerkelijk heeft getroffen, dan kan hij niet aan deze wettelijke verplichting voldoen. Ook kan hij ten onrechte veronderstellen dat de bewerker bepaalde beveiligingsmaatregelen heeft getroffen, wat kan leiden tot verlies of onrechtmatige verwerking van de verwerkte persoonsgegevens.
- *Onvoldoende transparantie over opgetreden beveiligingsincidenten*

[97] Artikel 14 lid 3 sub b Wbp.
[98] Een hostingprovider stelt webruimte ter beschikking aan partijen die een website op het internet willen plaatsen en die geen gebruik kunnen of willen maken van een eigen webserver.

Als de bewerker de verantwoordelijke niet tijdig en adequaat informeert over opgetreden beveiligingsincidenten, dan kan dat tot gevolg hebben dat de betreffende persoonsgegevens onrechtmatig worden verwerkt. Als een hostingprovider de verantwoordelijke bijvoorbeeld niet informeert over een inbraak in diens online database met creditcardgegevens, dan kan de verantwoordelijke vervolgens de betrokkenen niet informeren en zullen de betrokkenen hun creditcard pas laten blokkeren wanneer ze constateren dat er ten onrechte bedragen van hun rekening worden afgeschreven. Dit stelt de dief onnodig lang in staat om te frauderen met de gestolen creditcardgegevens.

Naast onvoldoende beveiliging en onvoldoende transparantie kan het aanpassen of staken van de dienstverlening onder meer leiden tot verlies van de verwerkte persoonsgegevens:

- *Onvoldoende continuïteit van de dienstverlening door de bewerker*
  Overname of faillissement van de bewerker kunnen ertoe leiden dat de bewerker zijn dienstverlening aanpast of staakt. Het gevolg kan onder meer zijn dat de persoonsgegevens die de bewerker verwerkte tijdelijk of permanent niet meer toegankelijk zijn voor de verantwoordelijke.
- *Onvoldoende portabiliteit van de verwerkte persoonsgegevens*
  Bewerkers maken bij het verwerken van persoonsgegevens niet altijd gebruik van standaardtechnologieën en -oplossingen. Door de bewerker verwerkte persoonsgegevens kunnen daardoor niet altijd zonder meer overgebracht worden naar een database van een andere bewerker of van de verantwoordelijke zelf. Als de bewerker zijn dienstverlening staakt, kan dit betekenen dat de verwerkte persoonsgegevens verloren gaan.

Praktijkvoorbeeld: Faillissement clouddienstverlener

Onderstaand praktijkvoorbeeld illustreert de dreiging van onvoldoende continuïteit van de dienstverlening door de bewerker.

Een Nederlandse clouddienstverlener biedt een aantal huisartseninformatiesystemen aan. Afnemers van de diensten kunnen deze informatiesystemen gebruiken om op de servers van het bedrijf hun patiëntendossiers bij te houden. Honderden huisartsenpraktijken en zorgcentra maken gebruik van deze diensten en in totaal beheert de dienstverlener zo"n anderhalf tot twee miljoen elektronische patiëntendossiers.
Als de dienstverlener failliet dreigt te gaan, ontstaat er onder de afnemers van de diensten grote onrust. Niet alleen zijn de klanten bang dat ze niet meer bij hun gegevens kunnen, maar ook de communicatie met verzekeraars over registraties en declaraties dreigt te stagneren als de huisartseninformatiesystemen niet meer beschikbaar zijn. Een aantal klanten van de dienstverlener, tevens lid van gebruikersverenigingen van de betreffende systemen, besluit in allerijl om de door de clouddienstverlener verwerkte gegevens elders onder te brengen. Ook Kamerleden maken zich zorgen, onder meer over wat er bij een eventuele overname met de patiëntgegevens gebeurt en wat dit betekent voor de privacy van de betrokkenen.
Uiteindelijk wordt er een passende overnamepartij gevonden.

Bewerkers kunnen bij het uitvoeren van hun dienstverlening gebruikmaken van de diensten van subbewerkers, die zelf ook weer bewerkers kunnen inschakelen. Bij bewerking door subbewerkers zijn de bovengenoemde dreigingen en kwetsbaarheden in versterkte mate aanwezig. Dit geldt in ieder geval voor:

- *Onvoldoende beveiliging door de subbewerker(s)*
  Om voor de verwerking als geheel te kunnen spreken van een adequaat beveiligingsniveau, moeten de bewerker en de eventuele subbewerkers de juiste beveiligingsmaatregelen treffen en moeten de beveiligingsmaatregelen gezamenlijk de belangrijkste dreigingen afdekken. Naarmate het aantal subbewerkers toeneemt, wordt ook de kans groter op lacunes in de beveiliging.[99]
- *Onvoldoende transparantie over de verwerking en de beveiliging door de subbewerker(s)*
  Om aan zijn wettelijke verplichtingen te kunnen voldoen moet de verantwoordelijke voldoende inzicht hebben in welke subbewerkers welke taken uitvoeren bij de verwerking en in het daarbij geboden beveiligingsniveau. Als hij hier niet voldoende inzicht in heeft of als hij niet vast kan stellen of alle subbewerkers de overeengekomen beveiligingsmaatregelen daadwerkelijk hebben getroffen, kan hij niet aan deze wettelijke verplichting voldoen. Ook kan hij dan ten onrechte

[99] Zie ook WP29, *Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker"*, p. 31-32: "De richtlijn belet geenszins dat om organisatorische redenen meerdere entiteiten als gegevensverwerker of (sub-)verwerker worden aangewezen of dat de desbetreffende taken worden onderverdeeld. Zij moeten zich echter allen bij de verwerking houden aan de opdrachten van de voor de verwerking verantwoordelijke. [...] Het strategische punt is hier dat – wanneer meerdere partijen bij het proces betrokken zijn – de verplichtingen en verantwoordelijkheden uit de wetgeving duidelijk behoren te worden belegd en niet versnipperd mogen raken over de keten van uitbesteding/onderaanneming." (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_nl.pdf).

veronderstellen dat een subbewerker bepaalde beveiligingsmaatregelen heeft getroffen, wat kan leiden tot verlies of onrechtmatige verwerking van de verwerkte persoonsgegevens.

Praktijkvoorbeeld: Stroomstoring bij een subbewerker

Onderstaand voorbeeld geeft weer hoe een bewerker afhankelijk kan zijn van een subbewerker.

Een clouddienstverlener biedt kantoorautomatiseringsapplicaties aan. Afnemers van de diensten kunnen met deze applicaties onder meer hun klantenbestand beheren. De gegevens worden opgeslagen in databases van de dienstverlener. Voor de opslag van de gegevens maakt de clouddienstverlener gebruik van de diensten van een subbewerker, een grote aanbieder van gegevensopslag in de cloud.
Een blikseminslag in een transformator in de buurt van een van de datacentra van de subbewerker veroorzaakt een explosie waarna brand uitbreekt, met als gevolg dat de subbewerker ook zijn noodgeneratoren niet op kan starten en de stroom volledig uitvalt. Doordat de servers van de subbewerker niet beschikbaar zijn, kunnen ook de kantoorautomatiseringsapplicaties van de clouddienstverlener een aantal uren niet worden gebruikt. Uiteindelijk blijkt de schade bij de subbewerker zo groot te zijn dat deze er niet in slaagt om alle gegevens terug te halen.

Naast de verwerking door subbewerkers is een tweede aandachtspunt de verwerking van persoonsgegevens buiten Nederland. Hiervan is sprake in de volgende situaties:
- *Bewerker (deels) buiten Nederland*
  De verantwoordelijke stelt persoonsgegevens ter beschikking aan een bewerker die is gevestigd buiten Nederland of die een of meer vestigingen heeft buiten Nederland, om deze gegevens daar door de bewerker te laten verwerken.
- *Subbewerker (deels) buiten Nederland*
  De bewerker stelt persoonsgegevens ter beschikking aan een subbewerker die is gevestigd buiten Nederland of die een of meer vestigingen heeft buiten Nederland, om deze gegevens daar door de subbewerker te laten verwerken.
- *Cloud computing met gegevensopslag buiten Nederland*
  De verantwoordelijke, de bewerker of een of meer subbewerkers maken gebruik van cloud computing, waarbij persoonsgegevens worden opgeslagen buiten Nederland.

Bij verwerking van persoonsgegevens buiten Nederland moet in de risicoanalyse rekening worden gehouden met het volgende:
- *Niet-naleving van de Wbp*
  De Wbp bevat regels voor doorgifte van persoonsgegevens aan landen buiten de Europese Unie. Het is aan de verantwoordelijke om te zorgen dat deze worden nageleefd.[100] De regels voor doorgifte van persoonsgegevens vallen buiten het bestek van deze richtsnoeren.[101]
- *Onvoldoende beveiliging, transparantie, continuïteit en/of portabiliteit*
  Bij verwerking van persoonsgegevens buiten Nederland kunnen alle eerder in deze paragraaf genoemde dreigingen en kwetsbaarheden in versterkte mate aanwezig zijn. Dit geldt met name voor de mate waarin de verantwoordelijke vast kan stellen of afgesproken beveiligingsmaatregelen daadwerkelijk zijn getroffen. De geografische afstand kan dusdanig zijn dat de verantwoordelijke dit niet zelf kan onderzoeken, waardoor hij afhankelijk wordt van voldoende gekwalificeerde, lokale partijen die dit namens hem vast kunnen stellen.

4.2 Afspraken in de bewerkersovereenkomst

De verantwoordelijke stelt vast welke beveiligingsmaatregelen de bewerker moet treffen om aan de betrouwbaarheidseisen te voldoen en op welke wijze de verantwoordelijke toeziet op naleving.
De afspraken hierover legt hij vast in de overeenkomst met de bewerker.

"[De verantwoordelijke] draagt zorg dat [de bewerker] voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen."[102]
"De verantwoordelijke draagt zorg dat de bewerker de persoonsgegevens verwerkt in overeenstemming met artikel 12, eerste lid en de verplichtingen nakomt die op de verantwoordelijke rusten ingevolge artikel 13."[103]

[100] Artikel 76, 77 en 78 Wbp.
[101] Meer informatie is beschikbaar op de website van het CBP. CBP, *Regels voor doorgifte van persoonsgegevens* (http://www.cbpweb.nl/Pages/th_doo_regels.aspx).
[102] Artikel 14 lid 1 Wbp.
[103] Artikel 14 lid 3 Wbp.

"De uitvoering van verwerkingen door een bewerker wordt geregeld in een overeenkomst of krachtens een andere rechtshandeling waardoor een verbintenis ontstaat tussen de bewerker en de verantwoordelijke."[104]
"Met het oog op het bewaren van het bewijs worden de onderdelen van de overeenkomst of de rechtshandeling die betrekking hebben op de bescherming van persoonsgegevens, alsmede de beveiligingsmaatregelen als bedoeld in artikel 13 schriftelijk of in een andere, gelijkwaardige vorm vastgelegd."[105]

Bij de beoordeling hanteert het CBP de volgende uitgangspunten:
- *Beveiligingseisen in de bewerkersovereenkomst*[106]
  Er is een bewerkersovereenkomst waarin alle relevante afspraken zijn vastgelegd over de beveiligingsmaatregelen die de bewerker moet treffen en over de wijze waarop de verantwoordelijke toeziet op naleving.
- *Differentiatie van de verwerkte persoonsgegevens*[107]
  Het kan voorkomen dat niet alle persoonsgegevens die de bewerker verwerkt even gevoelig zijn en dat niet voor alle verwerkte persoonsgegevens dezelfde afspraken van toepassing zijn. In de bewerkersovereenkomst is in dergelijke gevallen vastgelegd welke afspraken van toepassing zijn op welke persoonsgegevens.

Praktijkvoorbeeld: Noodstroomvoorziening en afspraken in het bewerkerscontract

Onderstaand voorbeeld illustreert hoe specifieke afspraken in de bewerkersovereenkomst de dienstverlening door de bewerker kunnen beïnvloeden.

Een datacentrum wordt getroffen door een stroomstoring, die iets minder dan drie kwartier duurt. Het datacentrum beschikt over verschillende noodstroomvoorzieningen in de vorm van een *uninterruptible power supply* (UPS) en dieselaggregaten. In een van de datahallen verloopt de overgang op noodstroom niet helemaal soepel: de batterijen van de noodstroomvoorziening houden er na zes seconden mee op en het duurt twintig seconden voordat het dieselaggregaat is aangeslagen.
Een aantal websites dat gebruikmaakt van servers in de getroffen datahal is na veertien seconden weer online. Bij andere klanten, waaronder een groot sociaal netwerk, duurt dit aanzienlijk langer. Het verschil wordt bepaald door de afspraken die de klanten in het bewerkerscontract hebben gemaakt over de noodstroomvoorziening. Websites van klanten die hebben gekozen voor een zogenoemde dubbele voeding komen weer online op het moment dat het dieselaggregaat aanslaat; de overige klanten moeten handmatig worden overgezet op noodstroom en voor hen duurt de storing ruim een uur.

Bij de beoordeling van de afspraken in de bewerkersovereenkomst betrekt het CBP in ieder geval de volgende onderwerpen:
- *De dienstverlening door de bewerker*
  Omschrijving van de dienst(en) die de bewerker verleent en de persoonsgegevens die de bewerker daarbij verwerkt (eventueel gedifferentieerd op basis van gevoeligheid). Verder wordt omschreven welke (groepen) medewerkers van de bewerker toegang hebben tot welke persoonsgegevens en welke handelingen deze medewerkers uit mogen voeren met de persoonsgegevens. Er is een expliciet verbod opgenomen om andere handelingen met de persoonsgegevens uit te voeren dan wat hier is omschreven.
- *De betrouwbaarheidseisen die op de verwerking van toepassing zijn*
  Weergave van de betrouwbaarheidseisen die op de verwerking van toepassing zijn, waar van toepassing gedifferentieerd op basis van de gevoeligheid van de verwerkte persoonsgegevens.
- *De beveiliging door de bewerker*
  Afspraken over de technische en organisatorische beveiligingsmaatregelen waarmee de bewerker invulling geeft aan de betrouwbaarheidseisen. Deze maatregelen liggen in het verlengde van de beveiligingsmaatregelen die de verantwoordelijke moet treffen. Deze worden nader toegelicht in paragraaf 3.2 van deze richtsnoeren.[108]
- *Transparantie over de beveiliging*
  Afspraken over de inhoud en de frequentie van de rapportages die de bewerker aan de verant-

[104] Artikel 14 lid 2 Wbp.
[105] Artikel 14 lid 5 Wbp.
[106] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 6.2.3.
[107] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 7.2.
[108] Bij gebruik van specifieke vormen van dienstverlening kunnen aanvullende afspraken in het bewerkerscontract noodzakelijk zijn. Zie bijvoorbeeld voor afspraken over (technische) beveiligingsmaatregelen in bewerkersovereenkomsten met betrekking tot cloud computing: ENISA, *Procure Secure – A guide to monitoring of security service levels in cloud contracts* (http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts).

woordelijke oplevert over de beveiliging; omschrijving van het recht van de verantwoordelijke om de naleving van de beveiligingsmaatregelen door onafhankelijke deskundigen vast te laten stellen. Onafhankelijke deskundigen kunnen bijvoorbeeld it-auditors of penetratietesters zijn.
- *Transparantie over opgetreden beveiligingsincidenten*
  Afspraken over de inhoud van rapportages over beveiligingsincidenten en datalekken, de criteria voor rapportage van incidenten en de snelheid waarmee wordt gerapporteerd. In de afspraken is opgenomen dat de bewerker beveiligingsincidenten en datalekken die (mogelijk) gevolgen hebben voor betrokkenen meteen rapporteert en dat de bewerker waar nodig ook meewerkt aan het adequaat informeren van de betrokkenen.
- *Verwerking door subbewerkers*
  Afspraken over het al dan niet toestaan van verwerking door subbewerkers, met daarbij de eventuele beperkingen. Beperkingen zijn bijvoorbeeld dat de bewerker subbewerkers mag inschakelen maar dat de subbewerkers geen subsubbewerkers in mogen schakelen of dat bij de verwerking van specifieke klassen van persoonsgegevens geen subbewerkers mogen worden ingeschakeld.
  Als bewerking door subbewerkers is toegestaan, dan is in de bewerkersovereenkomst opgenomen dat met de subbewerkers overeenkomsten moeten worden afgesloten en dat alle verplichtingen uit het bewerkerscontract die relevant zijn voor de beveiliging van de verwerkte persoonsgegevens daarin moeten worden overgenomen.
- *Verwerking van de persoonsgegevens buiten Nederland*
  Afspraken over welke persoonsgegevens in welke landen worden verwerkt.
- *Voorwaarden voor heronderhandeling of beëindiging van de overeenkomst*

Afspraken over heronderhandeling van de bewerkersovereenkomst als een wijziging in de verwerkte persoonsgegevens of in de betrouwbaarheidseisen daar aanleiding toe geeft. Bij de afspraken is ook een noodplan opgenomen voor het geval een van de partijen de relatie wil beëindigen voor het einde van de looptijd van de overeenkomst. Verder is vastgelegd hoe en in welke vorm de verantwoordelijke de verwerkte persoonsgegevens weer ter beschikking krijgt en hoe wordt geborgd dat de bewerker na het beëindigen van de relatie niet meer over de persoonsgegevens kan beschikken.

Zoals aangegeven moet de bewerker als hij gebruikmaakt van subbewerkers, met deze subbewerkers overeenkomsten afsluiten. In deze overeenkomsten moeten bovengenoemde onderwerpen worden afgedekt en moeten alle bepalingen uit het bewerkerscontract worden overgenomen die relevant zijn voor de beveiliging van de verwerkte persoonsgegevens.

Bewerkers die gevestigd zijn buiten de eu of die persoonsgegevens verwerken buiten de eu, hebben in veel gevallen maatregelen getroffen om de doorvoer van persoonsgegevens vanuit de eu mogelijk te maken. Een voorbeeld van een dergelijke maatregel, die door Amerikaanse bedrijven wordt gebruikt, is certificering van de bewerker op basis van het Safe Harbor-raamwerk.[109] Deze maatregelen worden getroffen in aanvulling op bovenstaande beveiligingsmaatregelen en vormen op zichzelf geen waarborg voor de adequate beveiliging van de verwerkte persoonsgegevens. Evenmin biedt de Safe Harbor-certificering zekerheid over de waarborgen bij de eventuele subbewerkers.

4.3 Toezicht op naleving van de afspraken

De verantwoordelijke stelt vast dat de afspraken in de bewerkersovereenkomst daadwerkelijk worden nageleefd.

"De verantwoordelijke ziet toe op de naleving van [de technische en organisatorische beveiligingsmaatregelen door de bewerker]."[110]

Bij de beoordeling van het toezicht op naleving van de gemaakte afspraken onderkent het CBP in ieder geval de volgende kernpunten:
- *Controle en beoordeling van de dienstverlening door de bewerker*[111]
  De verantwoordelijke stelt vast dat de afspraken uit de bewerkersovereenkomst daadwerkelijk worden nageleefd. Hij stelt in ieder geval vast dat de bewerker overeengekomen rapportages daadwerkelijk levert en beoordeelt deze ook inhoudelijk. Verder maakt hij om voldoende zekerheid te krijgen over de naleving gebruik van bijvoorbeeld audits of andere onderzoeken door onafhankelijke partijen.
- *Beoordeling en afhandeling van beveiligingsincidenten en datalekken*[112]

[109] Export.gov, *U.S.-EU Safe Harbor* (http://export.gov/safeharbor/eu/index.asp).
[110] Artikel 14 lid 1 Wbp.
[111] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 10.2.2.
[112] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 13.1.2.

De verantwoordelijke beoordeelt de beveiligingsincidenten en datalekken die worden gerapporteerd door de bewerker of door eventuele subbewerkers. Datalekken die onder een wettelijke meldplicht vallen, meldt hij bij de betreffende toezichthouder. Als hij daartoe wettelijk verplicht is of als er anderszins aanleiding voor is, informeert hij ook de betrokkenen over het beveiligingsincident of het datalek.

- *Beheer van wijzigingen in de dienstverlening door de bewerker*[113]
  De verantwoordelijke stelt periodiek vast dat de beveiligingsmaatregelen die met de bewerker zijn overeengekomen nog steeds aantoonbaar overeenstemmen met de betrouwbaarheidseisen en neemt het initiatief tot aanpassing als dat niet meer het geval is. Van wijzigingen die de bewerker initieert stelt de verantwoordelijke vast dat na implementatie nog steeds aan de betrouwbaarheidseisen wordt voldaan.

Nader bekeken: Controle en beoordeling van de dienstverlening door de bewerker

Effectieve controle en beoordeling van de dienstverlening vereisen een samenspel tussen twee partijen: de verantwoordelijke, die daadwerkelijk moet controleren en beoordelen, en de bewerker, die de verantwoordelijke daartoe de mogelijkheid moet bieden. Naast rapportages door de bewerker en onderzoek door een onafhankelijke derde in opdracht van de verantwoordelijke, staat beide partijen daarbij nog een aantal andere instrumenten ter beschikking. Deze instrumenten worden onderstaand toegelicht.

Het eerste instrument is de Third Party Mededeling (TPM). Een TPM is een verklaring van een onafhankelijke externe deskundige, waarin deze een oordeel geeft over de maatregelen die een bewerker heeft getroffen. De TPM wordt opgesteld in opdracht van de bewerker en wordt verstrekt aan de verantwoordelijken die gebruikmaken van de diensten van de bewerker. Het doel van het verstrekken van een TPM is om de verantwoordelijken inzicht te bieden in de getroffen maatregelen, zonder dat iedere verantwoordelijke daar zelf onderzoek naar hoeft te (laten) doen. Afspraken over te verstrekken TPM"s worden vastgelegd in het bewerkerscontract.

Het tweede instrument is certificering. Certificering houdt in dat de maatregelen van de bewerker door een geaccrediteerde onafhankelijke externe deskundige worden getoetst aan een norm. Relevante normen in dit verband zijn NEN-ISO/IEC 27001:2005 nl, die betrekking heeft op de wijze waarop de bewerker de informatiebeveiliging stuurt en beheerst, en NEN-ISO-IEC 20000-1:2011 en, die betrekking heeft op de sturing en beheersing van de dienstverlening door de bewerker. Certificering vindt plaats op initiatief van de bewerker. Als de verantwoordelijke dit instrument in wil zetten, kiest hij voor een bewerker die tegen de relevante norm(en) is gecertificeerd.

Het is aan de verantwoordelijke om voor zijn specifieke situatie vast te stellen hoe veel zekerheid hij aan het gebruik van deze instrumenten kan ontlenen en of hij met alle middelen die hij tot zijn beschikking heeft in staat is om te voldoen aan zijn wettelijke verplichting om toezicht te houden op de naleving van de technische en organisatorische beveiligingsmaatregelen door de bewerker.

4.4 Evaluatie en aanpassing van verwerking door een bewerker

De verantwoordelijke voert periodiek een evaluatie uit van de bewerking door een bewerker en past deze bewerking waar nodig aan. Als zich tussentijds grote veranderingen voordoen, beoordeelt hij deze en voert hij de eventueel noodzakelijke aanpassingen door.

De verantwoordelijke stelt periodiek, of wanneer de omstandigheden daar aanleiding toe geven, vast of er nog steeds sprake is van "voldoende waarborgen [...] ten aanzien van de technische en organisatorische beveiligingsmaatregelen"[114] en of de bewerker nog steeds "de verplichtingen nakomt die op de verantwoordelijke rusten ingevolge artikel 13."[115] Waar nodig voert hij aanpassingen door.

Bij grote veranderingen in de dienstverlening door de bewerker en eventuele subbewerkers stelt de verantwoordelijke vast of de gemaakte afspraken nog steeds toereikend zijn. Van dergelijke veranderingen is bijvoorbeeld sprake als de bewerker wordt overgenomen of een ingrijpende aanpassing doorvoert in zijn algemene voorwaarden. Ook grote veranderingen bij de verantwoordelijke zelf kunnen hier aanleiding toe geven, bijvoorbeeld als in de nieuwe situatie de persoonsgegevens die de bewerker verwerkt veel gevoeliger zijn dan voorheen het geval was.
Het aanbod aan dienstverlening kan in de loop van de tijd veranderen en ook kunnen de ervaringen die de verantwoordelijke met de bewerker heeft opgedaan aanleiding zijn om voor een andere

[113] Deze maatregel wordt nader uitgewerkt in NEN-ISO/IEC 27002:2007 nl, paragraaf 10.2.3.
[114] Artikel 14 lid 1 Wbp.
[115] Artikel 14 lid 3 Wbp.

bewerker of een andere vorm van dienstverlening te kiezen. Verder kan de aard van de verwerking of van de verwerkte persoonsgegevens in de loop van de tijd leiden tot nieuwe of andere risico"s voor de betrokkenen, bijvoorbeeld als gevolg van maatschappelijke ontwikkelingen. De verantwoordelijke voert daarom een periodieke evaluatie uit en kiest op basis daarvan zo nodig voor een andere bewerker, een andere vorm van dienstverlening of voor aanscherping van de afspraken in het bewerkerscontract. Bij dit laatste neemt de verantwoordelijke ook de getrokken lessen uit de opgetreden beveiligingsincidenten mee.

5 HANDHAVING EN DE ROL VAN HET CBP

Verantwoordelijken die in strijd handelen met het bepaalde in de Wbp kunnen op verschillende manieren in rechte worden aangesproken, zowel civiel-, bestuurs- als strafrechtelijk. Betrokkenen hebben een aantal mogelijkheden om zelf hun recht te halen, zowel op grond van de Wbp als op grond van het algemene bestuursrecht en het civiele recht. Daarnaast heeft het CBP als toezichthouder een aantal bestuursrechtelijke mogelijkheden om te handhaven op het bepaalde in de Wbp.

5.1 Maatregelen door betrokkenen

Waar van toepassing kunnen betrokkenen zelf een belangrijke bijdrage leveren aan de beveiliging van hun persoonsgegevens, bijvoorbeeld door te kiezen voor sterke (moeilijk te raden) wachtwoorden en door gebruikte apparatuur voldoende te beveiligen. Betrokkenen die menen dat hun persoonsgegevens onvoldoende worden beveiligd, kunnen actie ondernemen door hun vraag of klacht voor te leggen aan de verantwoordelijke. Verder kunnen zij gebruikmaken van het recht op inzage, correctie, verwijdering en verzet.[116] Het recht op inzage en correctie kan betrokkenen helpen bij het achterhalen en laten corrigeren van fouten of onvolledigheden in hun persoonsgegevens. Het recht op verwijdering en verzet geeft betrokkenen onder bepaalde voorwaarden de mogelijkheid om zich te onttrekken aan verwerkingen die voor hen risicovol zijn. Het CBP heeft op www.mijnprivacy.nl concrete hulpmiddelen voor betrokkenen gepubliceerd, waaronder voorbeeldbrieven aan verantwoordelijken.

Als een verantwoordelijke zich niet houdt aan het bepaalde in de Wbp, kan een betrokkene ook zelf de rechter vragen om een verbod op te leggen op het verder verwerken van bepaalde persoonsgegevens[117] of om hem/haar een schadevergoeding toe te kennen.[118]

De Wbp biedt betrokkenen daarnaast in een aantal specifieke gevallen (onder meer bij weigering van inzage in persoonsgegevens en bij weigering van een verzoek tot verbetering, aanvulling of verwijdering van gegevens) de mogelijkheid een verzoekschrift in te dienen bij de rechtbank, mits de verantwoordelijke een bedrijf of een burger is.
Als de verantwoordelijke een bestuursorgaan is, zijn de bezwaar- en beroepsregels uit de Algemene wet bestuursrecht (Awb) van toepassing.

5.2 Handhaving door het CBP

Het CBP heeft de wettelijke taak om toe te zien op de naleving van de Wbp.[119] Daartoe beschikt het CBP over een aantal middelen.

De signalen die het CBP ontvangt via de signaalfunctie op www.mijnprivacy.nl, het telefonisch spreekuur en per post geven een beeld van de naleving van de wettelijke regels die zien op de bescherming van persoonsgegevens en kunnen voor het CBP aanleiding zijn om een onderzoek in te stellen.

Het CBP kan op grond van een klacht van een belanghebbende of op eigen initiatief een onderzoek instellen naar de naleving van de Wbp.[120] Daarbij kan het CBP zijn toezichthoudende bevoegdheden inzetten,[121] waarbij een verantwoordelijke verplicht is alle gevraagde medewerking te verlenen.
Het CBP kan inlichtingen vorderen, inzage vorderen in zakelijke gegevens, zaken en middelen onderzoeken (waaronder computerapparatuur) en ruimtes betreden, waaronder woningen.[122] Het aantal aangedragen zaken en de complexiteit daarvan neemt echter voortdurend toe, terwijl de middelen die het CBP ter beschikking staan begrensd zijn. Het CBP kan derhalve niet alle zaken die

[116] Artikelen 5, 35, 36, 37, 38, 39, 40 en 41 Wbp.
[117] Artikel 50 Wbp.
[118] Artikel 49 Wbp.
[119] Artikel 51 Wbp.
[120] Artikel 60 Wbp.
[121] Voor al zijn toezichthoudende activiteiten, niet alleen bij ambtshalve onderzoeken.
[122] Artikel 61 lid 2 Wbp jo. artikel 5:15 Awb.

worden aangebracht in behandeling nemen en moet keuzes maken. Het CBP geeft prioriteit aan zaken waarbij het een vermoeden heeft van ernstige, structurele overtredingen die veel mensen treffen en waarbij het CBP door de inzet van handhavingsinstrumenten effectief verschil kan maken.[123]

Indien de Wbp niet wordt nageleefd, kan het CBP bestuursdwang toepassen. Onder een last onder bestuursdwang wordt verstaan het met feitelijk handelen optreden door een bestuursorgaan tegen een illegale situatie, doorgaans op kosten van de overtreder. Ook kan het CBP een last onder dwangsom opleggen. Een last onder dwangsom kan bijvoorbeeld inhouden dat een verantwoordelijke bepaalde beveiligingsmaatregelen moet treffen binnen een vastgestelde termijn op straffe van een dwangsom van een bepaald bedrag per dag. Als de verantwoordelijke niet voldoet aan de last, kan het te betalen geldbedrag fors oplopen, tot een vooraf vastgesteld maximumbedrag.

Het CBP werkt bij onderzoeken naar overtredingen van de Wbp met een internationaal karakter samen met collega-toezichthouders binnen en buiten de eu.

[123] CBP, *Beleidsregels handhaving door het CBP* (http://www.cbpweb.nl/Pages/ind_cbp-beleidsregels-cbp.aspx).

BIJLAGE: TEKST VAN DE GECITEERDE WETSARTIKELEN

Deze bijlage bevat de volledige tekst van artikel 12, 13 en 14 Wbp.

1 Artikel 12 Wbp

1 Een ieder die handelt onder het gezag van de verantwoordelijke of van de bewerker, alsmede de bewerker zelf, voor zover deze toegang hebben tot persoonsgegevens, verwerkt deze slechts in opdracht van de verantwoordelijke, behoudens afwijkende wettelijke verplichtingen.
2 De personen, bedoeld in het eerste lid, voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit. Artikel 272, tweede lid, van het Wetboek van Strafrecht is niet van toepassing.

2 Artikel 13 Wbp

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 van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico"s die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

3 Artikel 14 Wbp

1 Indien de verantwoordelijke persoonsgegevens te zijnen behoeve laat verwerken door een bewerker, draagt hij zorg dat deze voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen. De verantwoordelijke ziet toe op de naleving van die maatregelen.
2 De uitvoering van verwerkingen door een bewerker wordt geregeld in een overeenkomst of krachtens een andere rechtshandeling waardoor een verbintenis ontstaat tussen de bewerker en de verantwoordelijke.
3 De verantwoordelijke draagt zorg dat de bewerker
   a de persoonsgegevens verwerkt in overeenstemming met artikel 12, eerste lid en
   b de verplichtingen nakomt die op de verantwoordelijke rusten ingevolge artikel 13.
4 Is de bewerker gevestigd in een ander land van de Europese Unie, dan draagt de verantwoordelijke zorg dat de bewerker het recht van dat andere land nakomt, in afwijking van het derde lid, onder b.
5 Met het oog op het bewaren van het bewijs worden de onderdelen van de overeenkomst of de rechtshandeling die betrekking hebben op de bescherming van persoonsgegevens, alsmede de beveiligingsmaatregelen als bedoeld in artikel 13 schriftelijk of in een andere, gelijkwaardige vorm vastgelegd.

Het College bescherming persoonsgegevens houdt onder de Wet bescherming persoonsgegevens toezicht op de naleving van wetten die het gebruik van persoonsgegevens regelen. Onduidelijkheid over wet- en regelgeving kan ten koste gaan van de bescherming van de gegevens van burgers. Daarom geeft het College in zijn Richtsnoeren ten behoeve van toepassing in de praktijk nadere invulling aan de geldende wettelijke normen.

Rechterlijke uitspraken kunnen naast wetswijzigingen, technische ontwikkelingen en praktijkervaringen aanleiding geven tot aanvulling of herziening van deze richtsnoeren. Deze richtsnoeren treden in werking met ingang van 1 maart 2013, zijnde de datum van publicatie in de Staatscourant.