



Beveiliging van bestanden

In de Wbp wordt een persoonsgegeven als volgt gedefinieerd: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 1). Hieronder wordt deze categorie gegevens onderverdeeld in:

- direct herleidbare persoonsgegevens: persoonsgegevens die direct naar de identiteit van een persoon kunnen leiden. Dit betreft bijvoorbeeld NAW gegevens of email gegevens.
- indirect herleidbare persoonsgegevens: gegevens die in combinatie met een zogenaamde identifier met enige moeite (bv via een database die op een bekende locatie aanwezig is) zijn te herleiden tot de identiteit van een persoon. Een cliëntnummer is een identifier.

Gegevens die niet gerelateerd zijn aan personen worden 'gewone' gegevens genoemd.

'Anonieme gegevens' wordt hieronder als begrip niet gebruikt omdat dit kan leiden tot misverstanden: het begrip kan namelijk verwijzen naar indirect herleidbare gegevens als naar gewone gegevens.

Niet herleidbare (persoons)gegevens zijn gegevens die ook niet met een identifier kunnen worden herleid naar een persoon en zijn op dat moment dan ook te beschouwen als een gewoon gegeven.

In het uitvoeringsproces van een CQI meting worden op tal van momenten bestanden aangemaakt, opgeslagen, verwerkt, verstuurd, gemuteerd, samengevoegd, gesplitst, veranderd en vernietigd. Al deze handelingen worden in het kader van de Wbp "verwerkingen" genoemd. De bestanden en de verwerkingen dienen te worden beveiligd om verlies van data en onrechtmatige verwerking te voorkomen. De meetorganisatie dient daartoe beveiligingsmaatregelen te treffen. Artikelen 13 en 14 van de Wbp zijn belangrijke artikelen in dit verband.

Artikel 13 Wbp luidt :

"De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand 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."

Artikel 14 verplicht de Verantwoordelijke om de beveiligingsvoorschriften op te leggen aan de Bewerker en er op toe te zien dat bij de bewerker alleen die personen toegang hebben tot de gegevens die deze nodig hebben voor de uitvoering van hun taak. Daarom wordt in de schriftelijke bewerkersovereenkomst expliciet ingegaan op de beveiliging.

De "verantwoordelijke" is bij een CQI meting de opdrachtgever.

In de bewerkersovereenkomst wordt contractueel overeengekomen dat de meetorganisatie voldoende beveiligingsmaatregelen treft opdat voldaan wordt aan artikel 13.

De beveiligingsmaatregelen kunnen onder meer betrekking hebben op:

- de bestanden zelf
- de computer en het interne ICT netwerk waarop de bestanden worden verwerkt
- informatiedragers waar bestanden zijn opgeslagen w.o. (harddisks van) computers en laptops, CD roms, USB sticks, servers etc.
- de ruimte waar de informatiedragers zich bevinden (bv. serverruimte)
- externe ruimtes waar back up bestanden zich bevinden
- het externe netwerk dat gebruikt wordt voor transport / email van bestanden bijvoorbeeld internet



Accreditatierichtlijn Beveiliging van bestanden

Versie: 6.0
d.d. : juni 2010

- de werkplek en de ruimte waarin de werkplek is ondergebracht
- het toegangsbeheer en de personen die gerechtigd zijn om de bestanden te bewerken
- en andere onderdelen van het verwerkingssysteem
- het wel of niet verzenden van (persoons)gegevens per e-mail
- wijze van verzenden

De beveiliging van bestanden gezien vanuit de Wbp heeft als doel: de persoonsgegevens te vrijwaren tegen verlies en onrechtmatige verwerking en gelet op de doelen waarvoor deze worden verwerkt, deze niet langer dan noodzakelijk te verwerken in een vorm die te herleiden is naar de identiteit van een persoon. Normenkader paragraaf 2.2. behandelt vertrouwelijkheid van onderzoek en in ISO 20252 (paragraaf 3.3, 4.7.2, 4.9.3 en 4.9.2) wordt gesproken over o.a. het voorkomen van verlies en beschadiging van bestanden en worden eisen genoemd voor virusprotectie, opslag en veilige bewaring. In deze richtlijn zijn de eisen van de Wbp, het normenkader en ISO 20252 geïntegreerd.

Vernietiging van bestanden die persoonsgegevens bevatten is een belangrijk aandachtspunt in de Wbp. Deze bestanden mogen niet langer bewaard worden dan noodzakelijk. In het CKZ handboek en verschillende richtlijnen worden de momenten van vernietiging binnen het proces beschreven. In de regel is dat direct na gebruik tenzij er een kans bestaat dat het bestand op een later moment nog moet worden ingezien. Alle bestanden met persoonsgegevens dienen binnen een week nadat de meetorganisatie heeft aangegeven dat het opgeleverde bestand voldoet om de meetwerkzaamheden uit te voeren, te worden vernietigd. De meetorganisatie moet uiterlijk binnen twee weken na ontvangst van het bestand melden of het bestand voldoet. Indien er binnen drie weken na oplevering van de bestanden geen bericht is ontvangen van de meetorganisatie wordt het (de) bron bestand(en) daarna binnen een week vernietigd.



Drie beveiligingsniveaus voor bestanden

In het verlengde van de het Cbp-document “beveiliging van persoonsgegevens” (AV23, cpbweb) worden drie niveaus van beveiliging onderscheiden:

1. Basisniveau beveiliging

Het basisniveau van beveiliging geldt voor alle (bewerkingen die worden uitgevoerd met) bestanden met risicoklasse 1. Dit zijn bestanden met gewone gegevens. Voor het basisniveau van beveiliging volstaat de standaard beveiliging die ook noodzakelijk zijn voor een zorgvuldige bedrijfsvoering. Hiertoe behoren o.a. toegangsrechten conform de normale procedures, beveiligde ICT infrastructuur (tegen virussen en ander malware en ongewenst binnendringen van onbevoegden), fysieke beveiliging van opbergkasten, beveiliging serverruimtes, back up procedures, fysieke beveiliging van het gebouw en gebruikelijke eisen aan emailverkeer, beveiligd inkiezen vanuit locaties op afstand (bv thuiscomputers en laptops op afstand). Er wordt alleen gewerkt met legaal verkregen softwareapplicaties waarbij sprake is van gecontroleerd onderhoud door een intern verantwoordelijke.

In richtlijnen op gebied van informatiebeveiliging of in het hierboven genoemde document AV23 kunnen desgewenst aanvullende maatregelen worden gevonden.

Bij CQI metingen worden geen bestanden opgeslagen op losse informatiedragers zoals usb sticks, laptops, thuiswerkplekken, CD rom. Dit geldt ook voor bestanden met gewone gegevens, niet zijnde persoonsgegevens. Alle bestanden worden en blijven opgeslagen op het beveiligde ICT netwerk van de meetorganisatie. Deze eis vloeit niet voort uit de Wbp maar uit ISO 20252. Bestanden mogen alleen op thuiswerkplekken worden verwerkt (het opslaan van bestanden daartoe niet inbegrepen) als deze geen (direct of indirect herleidbare) persoonsgegevens bevatten en de informatiebeveiliging aan de ISO 20252 norm voldoet.

2. Verhoogd niveau beveiliging

Een verhoogd niveau van beveiliging geldt voor alle (verwerkingen die worden uitgevoerd met) bestanden met risicoklasse 2. Dit zijn bestanden waarin persoonsgegevens zijn opgenomen die direct of indirect te herleiden zijn tot de identiteit van een persoon. Verlies van deze gegevens of onzorgvuldige of onbehoorlijke verwerking leidt tot beperkte negatieve gevolgen voor de betrokkenen/respondenten. Bestanden waarin gegevens zijn opgenomen, over de gezondheid van de betrokkenen of respondenten, die zelfstandig of in combinatie met andere aanwezige gegevens kunnen leiden naar de identiteit van een persoon horen hier NIET toe. Deze vallen in risicoklasse 3. Het verhoogde niveau van beveiliging betreft een uitbreiding van het basisniveau van beveiliging plus een aantal aanvullende maatregelen of procedures:

- De toegangsrechten zijn beperkt tot alleen diegenen die de bestanden mogen inzien en bewerken. Er is dus sprake van exclusieve toegang. Vanwege de privacyeisen dient het aantal personen dat toegang krijgt tot het minimum beperkt te blijven. De bevoegdheidsstructuur wordt voorafgaand aan de uitvoering van het project geïmplementeerd en genoteerd in het interne logboek.
- De bestanden worden op een apart en afgeschermd deel van het ICT netwerk opgeslagen dat alleen toegankelijk is voor bevoegde personen.
- De bevoegden slaan de bestanden versleuteld op met behulp van encryptie op applicatieniveau (binnen excel bijvoorbeeld met behulp van een wachtwoord).
- De computers die zijn aangesloten op het netwerk loggen na een vastgesteld aantal minuten ‘niet gebruik’ automatisch uit.
- Printouts worden bewaard in afsluitbare kasten.
- Bestanden worden niet gebruikt of bewerkt op thuiscomputers.



- Indien een bestand met persoonsgegevens getransporteerd moet worden dan gebeurt dat in principe per (encrypted) email of via een SFTP verbinding (dus niet via fysiek transport op een losse informatiedrager).
- Bestanden met persoonsgegevens die worden verstuurd met email worden versleuteld met encryptie op applicatie niveau waarbij de encryptie sleutel apart wordt verzonden. Bestanden worden na verzending en ontvangst direct uit het emailprogramma verwijderd en opgeslagen op het afgeschermd gedeelte van het ICT netwerk.
- Server ruimte is fysiek beveiligd evenals de toegang tot het gebouw (inbraakbeveiliging).
- Externe back ups worden veilig versleuteld (d.w.z. encryptie met hoge graad van beveiliging).
- De projectbestanden (inclusief backups) worden binnen 5 werkdagen vernietigd als zij niet meer nodig zijn voor het project.
- Alle functionarissen die zijn betrokken bij het project hebben een geheimhoudingsverklaring ondertekend.

3. Hoog niveau beveiliging

Een hoog niveau van beveiliging geldt voor alle (bewerkingen die worden uitgevoerd met) bestanden met risicoklasse 3. Dit zijn bestanden met naast persoonsgegevens ook bijzondere persoonsgegevens (in dit geval gegevens over gezondheid). Verlies van deze gegevens of onzorgvuldige of onbehoorlijke verwerking leidt tot schade voor de betrokkenen/respondenten vanwege de gevoeligheid van gegevens.

Een hoog niveau van beveiliging betreft een uitbreiding van het verhoogde beveiligingsniveau plus een aantal aanvullende maatregelen of procedures:

- Bestanden worden veilig versleuteld opgeslagen op het ICT netwerk (encryptie in bijvoorbeeld excel is alleen veilig als er een aparte procedure wordt gevolgd)
- Er wordt gewerkt met veilige wachtwoorden (tenminste 6 cijfer/lettercombinaties)
- Bestanden die worden verstuurd met email worden versleuteld met veilige encryptie en de encryptie sleutel wordt via een ander medium verzonden (bv telefoon of mondeling). Er wordt zeker gesteld dat de bestanden worden ontvangen door de juiste persoon. Bestanden worden na verzending en ontvangst direct uit het emailprogramma verwijderd en opgeslagen op het afgeschermd gedeelte van het ICT netwerk.
- De meetorganisatie zelf initieert minimaal eens per jaar of na zes uitgevoerde CQI metingen onverwachte audits om naleving van de beveiligingseisen te controleren.

CQI bestanden en risicoklasse

In het handboek CQI metingen is een overzicht van bestanden opgenomen met een daarbij behorende risico classificatie. Dit overzicht dient de meetorganisatie te volgen bij het uitvoeren van de door haar gecontracteerde werkzaamheden.

Beveiliging papieren informatiedragers

Ook papieren informatiedragers worden in het kader van deze richtlijn gezien als bestand indien er persoonsgegevens op zijn afgedrukt. Een voorbeeld daarvan is het interviewrooster. Deze papieren informatiedragers moeten worden gemarkeerd met "vertrouwelijk". Ze dienen altijd aangetekend en beveiligd verstuurd te worden met openbare post of persoonlijk overhandigd aan een bevoegde. Printouts die niet meer worden gebruikt worden ontdaan van de persoonsgegevens en/of zo snel mogelijk vernietigd. Vernietiging gebeurt met behulp van een papiervernietiger. De meetorganisatie heeft voorts procedures geïmplementeerd en verantwoordelijkheden belegd die ervoor zorgen dat papieren informatiedragers met persoonsgegevens niet kunnen kwijtraken of onderwerp kunnen worden van onrechtmatige verwerking door onbevoegde derden.

Scheiding onderzoeksgegevens en communicatiegegevens



Accreditatierichtlijn Beveiliging van bestanden

Versie: 6.0
d.d. : juni 2010

In het proces van de CQI meting worden de gegevens die nodig zijn voor het onderzoek (zoals, geslacht, geboortedatum, AGB-code, DBC-code) zo snel en zoveel mogelijk gescheiden van de communicatiegegevens (gegevens die benodigd zijn voor de benadering van de respondenten waarbij een identifyer wordt toegevoegd voor koppeling later in het proces. In de steekproeftrekking wordt bijvoorbeeld gewerkt met een cliënten, populatie- en achtergrondbestand waar alleen maar onderzoeksgegevens in worden opgenomen met een identifyer (zoals cliëntnummer). Daarnaast wordt er een respondentenbestand aangemaakt dat alleen maar communicatiegegevens bevat. Ook bij de dataverzameling wordt deze scheiding aangebracht door middel van een identifyer (zoals een zogenaamd enquêtenummer).

Organisatorisch dient de meetorganisatie conform de instructies in het CQI handboek functiescheiding aan te brengen tussen medewerkers die de verschillende type bestanden gebruiken.

Onderzoeksgegevens dienen afgeschermd te worden van medewerkers die met communicatiegegevens werken en vice versa.