

NOREA Handreiking

Privacy Control Framework

**Template**  
  
Beheersingsdoelstellingen en beheersingsmaatregelen

voor privacy audits en privacy-assuranceopdrachten

Versie 2.0

Augustus 2019

**©2019 NOREA**, All rights reserved  
PO box 7984, 1008 AD Amsterdam  
phone: +3120-3010380  
e-mail: [norea@norea.nl](mailto:norea@norea.nl)  
[www.norea.nl](http://www.norea.nl)

Deel 3. Privacy Control Framework – Beheersingsmaatregelen

[Management 5](#_Toc10723858)

[Informeren 15](#_Toc10723859)

[Keuze en toestemming 16](#_Toc10723860)

[Verzamelen 18](#_Toc10723861)

[Inzage en kwaliteit van gegevens 24](#_Toc10723862)

[Verstrekken 29](#_Toc10723863)

[Gegevensbeveiliging 33](#_Toc10723864)

[Monitoren en handhaven 38](#_Toc10723865)

De volgende pagina’s geven een opsomming van de beheersingsmaatregelen van het PCF, geordend per onderwerp en per fase uit het levenscyclusmodel. Voor elk onderwerp wordt de beheersingsdoelstelling genoemd, evenals de gerelateerde kernelementen uit de AVG.

Voor elke beheersingsmaatregel is in een afzonderlijke kolom aangegeven of die maatregel van toepassing is voor een verwerkingsverantwoordelijke (‘VV’), verwerker (‘V’), of beide (‘VV, V’).

Management

|  |  |  |
| --- | --- | --- |
| Privacybeleid (PPO)  *Beheersingsdoelstelling:*  De entiteit stelt een privacybeleid vast en communiceert dit. Dit beleid bevat de doelstellingen en verantwoordelijkheden met betrekking tot privacy en is in overstemming met geaccepteerde privacyprincipes en de van toepassing zijnde wet- en regelgeving. | | |
| *Fase informatielevenscyclusmanagement:* **Management** | | |
| *Beheersingsmaatregelen:* | |  |
| PPO01 | De entiteit heeft een gedocumenteerd privacybeleid vastgesteld en heeft dit gecommuniceerd aan de interne medewerkers en externe belanghebbenden. Het privacybeleid wordt jaarlijks door het management geëvalueerd en goedgekeurd. | VV, V |
| PPO02 | Het management brengt zijn commitment (en verantwoordelijkheid voor) solide en rechtmatige privacyprincipes tot uitdrukking. | VV, V |
| PPO03 | Het privacybeleid bevat de doelstellingen van de entiteit met betrekking tot privacy en de bescherming van persoonsgegevens (zie ook DMI02 en ULI02), | VV, V |
| PPO04 | (a) De entiteit neemt bij elke verwerking van persoonsgegevens de algemeen geaccepteerde en wettelijke privacyprincipes in acht en legt vast op welke wijze hieraan wordt voldaan.  (b) De entiteit zorgt ervoor dat voor elke verwerking van persoonsgegevens gedocumenteerde instructies van contractuele partners vastgelegd zijn. | VV  V |
| PPO05 | De entiteit heeft criteria opgesteld en vastgelegd om aan te tonen dat elke verwerking van persoonsgegevens rechtmatig is. | VV, V |
| *Gerelateerde kernelementen van de AVG:*   * Privacyprincipes * Rechtmatigheid van de verwerking * Register van de verwerkingsactiviteiten | | |

|  |  |  |
| --- | --- | --- |
| Afbakening van rollen en verantwoordelijkheden (RRE)  *Beheersingsdoelstelling:*  De entiteit definieert duidelijke rollen en verantwoordelijkheden met betrekking tot de bescherming van persoonsgegevens en het behalen van privacydoelstellingen, en implementeert deze. | | |
| *Fase informatielevenscyclusmanagement:* **Management** | | |
| *Beheersingsmaatregelen:* | |  |
| RRE01 | De entiteit stelt bij elke verwerking van persoonsgegevens vast en documenteert of zij verwerker of verwerkingsverantwoordelijke is. | V, VV |
| ~~RRE02~~ | *Vervangen door RRE03(b).* |  |
| RRE03 | (a) In de gevallen dat de entiteit als verwerkingsverantwoordelijke optreedt, sluit deze een overeenkomst met de verwerkers waarin de verantwoordelijkheden van de verwerker met betrekking tot privacy zijn vastgelegd. Indien de entiteit als gezamenlijke verwerkingsverantwoordelijke optreedt, worden afspraken gemaakt met de andere verwerkingsverantwoordelijke.  (b) In de gevallen dat een entiteit optreedt als verwerker, is er een overeenkomst met de verwerkingsverantwoordelijke(n) waarin de verantwoordelijkheden van de verwerker met betrekking tot privacy zijn vastgelegd. Als verwerking verder wordt uitbesteed aan een subverwerker, is er een overeenkomst met de subverwerker waarin de verantwoordelijkheden van de subverwerker met betrekking tot privacy zijn vastgelegd. | VV  V |
| RRE04 | De entiteit belast een aangewezen persoon, zoals een privacy officer of functionaris voor gegevensbescherming (FG), met het coördineren van en toezicht houden op privacybescherming. De taken bevoegdheden en verantwoordelijkheden van deze persoon worden duidelijk omschreven en regelmatig herzien. | VV, V |
| RRE05 | De taken en verantwoordelijkheden van individuele medewerkers voor wat betreft de bescherming van persoonsgegevens en naleving van de privacyprincipes worden vastgesteld en gecommuniceerd. | VV, V |
| *Gerelateerde kernelementen van de AVG*:   * Privacyprincipes * Verantwoordelijkheden van verwerkingsverantwoordelijke en verwerker * Register van de verwerkingsactiviteiten * Functionaris voor gegevensbescherming * Doorgiften van persoonsgegevens aan derde landen of internationale organisaties | | |

|  |  |  |
| --- | --- | --- |
| Identificatie en classificatie van persoonsgegevens (PDI)  *Beheersingsdoelstelling:*  De entiteit heeft een duidelijk beeld van en documenteert welke persoonsgegevens worden opgeslagen en verwerkt. Persoonsgegevens worden geïdentificeerd en er wordt op de juiste wijze mee omgegaan.  In de maatregelen voor bescherming van persoonsgegevens wordt rekening gehouden met verschillen in de gevoeligheid van persoonsgegevens. Dit leidt tot identificatie van risico’s en compliance met wet- en regelgeving. | | |
| *Fase informatielevenscyclusmanagement:* **Management** | | |
| *Beheersingsmaatregelen:* | |  |
| PDI01 | De entiteit identificeert en documenteert verwerking van persoonsgegevens aan de hand van een gedocumenteerd proces, en classificeert deze gegevens als zodanig. Dit omvat tevens processen, systemen en derden die persoonsgegevens verwerken. | VV, V |
| PDI02 | De entiteit maakt duidelijk onderscheid tussen de verwerking van  (a) persoonsgegevens en (b) bijzondere categorieën van persoonsgegevens. | VV, V |
| PDI03 | De entiteit heeft een procedure opgesteld om te bepalen of bij bestaande of geplande verwerking van persoonsgegevens bijzondere categorieën van persoonsgegevens worden verwerkt. Als dit het geval is, wordt de rechtmatigheid van de (geplande) verwerking uitvoerig beoordeeld en gedocumenteerd en worden maatregelen getroffen om veilige verwerking volgens de geldende voorschriften te waarborgen. | VV |
| PDI04 | (a) De entiteit houdt een register bij van de verwerkingsactiviteiten met daarin de kenmerken van deze activiteiten (rechtsgrond, doel, categorieën van gegevens en betrokkenen, ontvangers, beveiligingsmaatregelen).  (b) De entiteit houdt een register bij van de verwerkingsactiviteiten die voor elke ververkingsverantwoordelijke worden uitgevoerd met daarin de kenmerken van deze activiteiten (contactgegevens van verwerkingsverantwoordelijken, doorgiften, beveiligingsmaatregelen). | VV  V |
| *Gerelateerde kernelementen van de AVG*:   * Register van de verwerkingsactiviteiten * Privacyprincipes * Beveiliging van de verwerking | | |

|  |  |  |
| --- | --- | --- |
| Risicomanagement (RMA)  *Beheersingsdoelstelling:*  De entiteit identificeert, beoordeelt en beperkt systematisch en periodiek de factoren die het behalen van de privacydoelstellingen in gevaar kunnen brengen. | | |
| *Fase informatielevenscyclusmanagement:* **Management** | | |
| *Beheersingsmaatregelen:* | |  |
| RMA01 | Er is een proces ingericht om:   1. periodiek gebeurtenissen en factoren te identificeren die het behalen van de privacydoelstellingen in gevaar brengen; 2. de gevolgen van deze gebeurtenissen en factoren en de kans dat zij plaatsvinden te beoordelen, om vervolgens een passende risicorespons en beheersingsmaatregelen te formuleren. | VV, V |
| ~~RMA02~~ | *Samengevoegd met RMA01.* |  |
| RMA03 | Wanneer nieuwe of gewijzigde privacyrisico's worden gesignaleerd, worden de privacyrisicobeoordeling en de risicobeheerstrategieën herzien en zo nodig bijgewerkt. | VV, V |
| RMA04 | Acceptatiecriteria voor privacyrisico’s worden vastgesteld, goedgekeurd, gedocumenteerd en toegepast. | VV, V |
| RMA05 | De entiteit brengt de beheersingsmaatregelen in kaart die nodig zijn om privacyrisico's te mitigeren en implementeert deze. De voortgang van de implementatie wordt gevolgd en beoordeeld. | VV, V |
| *Gerelateerde kernelementen van de AVG:*   * Gegevensbeschermingseffectbeoordeling * Gegevensbescherming door ontwerp / door standaardinstellingen | | |

|  |  |  |
| --- | --- | --- |
| Data protection impact assessments (PIA)  *Beheersingsdoelstelling:*  De privacy-gerelateerde effecten van nieuwe producten en diensten en het gebruik ervan binnen de entiteit worden op systematische wijze geïdentificeerd, beoordeeld en aangepakt. | | |
| *Fase informatielevenscyclusmanagement:* **Management** | | |
| *Beheersingsmaatregelen:* | | *Bevindingen/ toetsing:* |
| PIA01 | De entiteit beoordeelt aan de hand van een gedocumenteerd proces de effecten op privacybescherming van nieuwe of sterk gewijzigde processen, producten en diensten (DPIA). | VV |
| PIA02 | Bij de DPIA wordt vastgesteld:   1. de aard van de geplande verwerkingen; 2. hun doelstelling, noodzaak, en proportionaliteit; 3. de privacyrisico's die beoogde verwerkingen met zich meebrengen voor betrokkenen; 4. welke maatregelen moeten worden genomen om deze risico's te beperken. | VV |
| ~~PIA03~~ | *Samengevoegd met PIA02*. |  |
| PIA04 | Alle relevante belanghebbenden zijn bij de DPIA betrokken en de  specifieke richtlijnen van de toezichthoudende autoriteit ten aanzien van beoordelingscriteria worden nageleefd. | VV |
| PIA05 | De entiteit documenteert welke systemen en software persoonsgegevens verwerken en houdt bij welke wijzigingen hierin zijn doorgevoerd. | VV |
| PIA06 | Een verandermanagementproces is vastgesteld om ervoor zorg te  dragen dat de in de DPIA goedgekeurde privacymaatregelen zijn  geïmplementeerd voordat de wijziging wordt doorgevoerd. | VV |
| *Gerelateerde kernelementen van de AVG:*   * Gegevensbeschermingseffectbeoordeling | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Beheer van privacyincidenten en inbreuken (PIB)  *Beheersingsdoelstelling:*  De entiteit detecteert incidenten met betrekking tot privacy en handelt deze af. Op privacy-gerelateerde incidenten wordt adequaat gereageerd met het doel de gevolgen te beperken en er worden maatregelen genomen om toekomstige inbreuken te voorkomen. | | | |
| *Fase informatielevenscyclusmanagement:* **Management** | | | |
| *Beheersingsmaatregelen:* | | |  |
| PIB01 | De entiteit heeft een formeel, omvattend proces vastgesteld gericht op het beheer van privacyincidenten en inbreuken in verband met persoonsgegevens, waarin het volgende is vastgelegd:   1. De verantwoordelijkheid van medewerkers om de aangewezen  privacyofficer of FG in te lichten wanneer er sprake is van een  privacyincident of een mogelijke inbreuk in verband met  persoonsgegevens; 2. De privacyfunctionaris of FG (of, indien van toepassing de security officer) beoordeelt of het een privacygerelateerd incident betreft.  Indien er een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, documenteert de privacyfunctionaris de aard van de inbreuk, de gevolgen en, bij benadering, het aantal persoonsgegevensregisters en betrokkenen in kwestie. 3. De privacyfunctionaris of FG initieert en coördineert de nodige maatregelen en bepaalt welke personen hierbij betrokken dienen te worden en welke belanghebbenden moeten worden geïnformeerd (zoals de verwerkingsverantwoordelijke wanneer de entiteit de rol van verwerker heeft of de toezichthouder als de entiteit verwerkings-verantwoordelijke is). 4. De privacyfunctionaris of FG houdt toezicht op de voortgang van de corrigerende maatregelen en licht het management in (en, indien van toepassing, de verwerkingsverantwoordelijke en de teozichthouder). | | VV, V |
| ~~PIB02~~ | *Samengevoegd met PIB06.* | |  |
| PIB03 | Het proces bevat een duidelijke escalatieprocedure, gebaseerd op het type en/of de ernst van het incident, tot aan het inwinnen van juridisch advies en het inlichten van het hoogste management. In de procedure staan de criteria voor het opnemen van contact met rechtshandhavende-, toezichthoudende of andere autoriteiten. | | VV, V |
| PIB04 | (a) De entiteit heeft een beleid ten aanzien van het melden van inbreuk op de beveiliging. Dit zorgt ervoor dat de toezichthoudende autoriteit tijdig wordt ingelicht wanneer het waarschijnlijk is dat een inbreuk risico's voor de rechten en vrijheden van de natuurlijke persoon met zich meebrengt.  (b) De entiteit heeft een beleid ten aanzien van het melden van een inbreuk op de beveiliging. Dit zorgt ervoor dat de betreffende verwerkingsverantwoordelijke tijdig wordt ingelicht over een dergelijke (mogelijke) inbreuk. | | VV  V |
| PIB05 | (a) In het geval van een inbreuk wordt alle vereiste informatie met betrekking tot de inbreuk verzameld en gemeld aan de toezichthoudende autoriteit. Tot deze informatie behoren ook de oorzaak en mitigerende maatregelen.  (b) In het geval van een (mogelijke) inbreuk wordt alle vereiste informatie met betrekking tot de inbreuk verzameld en gemeld aan de verwerkingsverantwoordelijke voor de betreffende verwerking. Tot deze informatie behoren ook de oorzaak en mitigerende maatregelen. | | VV  V |
| PIB06 | De aangewezen privacy officer of FG is belast met de algehele verantwoorde-lijkheid voor de melding van de inbreuk. De privacy officer documenteert alle gemaakte overwegingen bij het bepalen van de meldplicht. | | VV, V |
| PIB07 | In de procedure voor beheer van privacyincidenten en -inbreuken staat dat, op basis van de evaluatie van incidenten/inbreuken, correcties en verbeteringen worden doorgevoerd, en dat de informatie wordt gebruikt in bewustwordingsprogramma's voor medewerkers. | | VV, V |
| PIB08 | In de procedure voor beheer van privacyincidenten en -inbreuken is het  volgende vastgelegd:   1. na elk beveiligingsincident en inbreuk met betrekking tot  persoonsgegevens ('datalekken') en elke grootschalige inbreuk in verband met persoonsgegevens wordt een formele incident- beoordeling uitgevoerd, waarbij indien nodig externe expertise  wordt ingeschakeld; 2. incidenten worden periodiek geëvalueerd en de noodzakelijke  verbeteringen worden geïdentificeerd op basis van:  * de onderliggende oorzaak van het incident; * incidentpatronen; * wijzigingen in de interne controle en wetgeving;  1. De resultaten van de periodieke evaluatie en voortgang van de  verbeteringen worden gerapporteerd aan en beoordeeld door het management. | | VV, V |
| PIB09 | De procedure voor beheer van inbreuken wordt ten minste eenmaal per jaar herzien en tevens kort na de implementatie van ingrijpende wijzigingen in systemen of procedures. | | VV, V |
| *Gerelateerde kernelementen van de AVG:*   * Inbreuk in verband met persoonsgegevens | | | |
| Competenties medewerkers (SCO)  *Beheersingsdoelstelling:*  Medewerkers die vanuit hun functie toegang hebben tot persoonsgegevens of processen beheren waarin persoonsgegevens worden verwerkt, beschikken over de benodigde competenties met betrekking tot privacy om hun taken naar behoren te kunnen vervullen. | | | |
| *Fase informatielevenscyclusmanagement:* **Management** | | | |
| *Beheersingsmaatregelen:* | |  | |
| SCO01 | De entiteit legt vast over welke competenties met betrekking tot privacy medewerkers die met persoonsgegevens werken moeten beschikken. De entiteit stelt legt daarnaast vast hoe deze competenties kunnen worden verworven (o.a. door trainingen). | VV, V | |
| SCO02 | De entiteit documenteert in hoeverre individuele medewerkers over deze competenties beschikken en heeft een procedure opgesteld om een gebrek aan vaardigheden aan te vullen. | VV, V | |
| SCO03 | De entiteit besteedt bij de werving en onboarding van nieuwe medewerkers die belast zijn met beveiliging van persoonsgegevens en compliance met privacyprincipes aandacht aan competenties met betrekking tot privacy. De omgang met privacy is een van de punten in individuele beoordelingsgesprekken. | VV, V | |
| SCO04 | Het management evalueert jaarlijks de toewijzing van personeel, budgetten en andere middelen aan het privacyprogramma. | VV, V | |
| *Gerelateerde kernelementen van de AVG:*   * Beveiliging van de verwerking * Privacyprincipes * Functionaris voor gegevensbescherming | | | |

|  |  |  |
| --- | --- | --- |
| Bewustwording en training medewerkers (SAT)  *Beheersingsdoelstelling:*  De medewerkers zijn voldoende op de hoogte van de privacywetgeving en -regelgeving, het privacybeleid en de richtlijnen binnen de organisatie, en hun verantwoordelijkheden met betrekking tot privacy De entiteit implementeert programma’s om bewustwording te bereiken en op peil te houden.. | | |
| *Fase informatielevenscyclusmanagement:* **Management** | | |
| *Beheersingsmaatregelen:* | | *Bevindingen/ toetsing:* |
| SAT01 | Ten minste eenmaal per jaar wordt voor alle medewerkers een bewustwordingscursus ten aanzien van privacy en beveiliging georganiseerd. Nieuwe medewerkers, contractanten en anderen wordt verplicht om binnen een maand na aanvang van de overeenkomst een vergelijkbare training te volgen, zodat zij op de hoogte zijn van het privacybeleid van de entiteit en de implicaties hiervan. | VV, V |
| SAT02 | Verdiepende (interne of externe) privacytraining wordt aangeboden op basis van de benodigde privacycompetenties van medewerkers (zie SCO). Tijdens de training worden het beleid en de procedures met betrekking tot privacy en relevant beveiligingsbeleid en -procedures behandeld, alsook overwegingen van wettelijke of regelgevende aard, de incidentrespons en gerelateerde onderwerpen.  Een dergelijke training is:   * jaarlijks verplicht voor alle medewerkers die toegang hebben tot persoonsgegevens of belast zijn met de bescherming ervan; * afgestemd op de verantwoordelijkheden van de medewerker binnen zijn of haar functie en de benodigde competenties. | VV, V |
| SAT03 | Trainingen en bewustwordingscursussen worden geëvalueerd en geactualiseerd om aan te sluiten bij de huidige wet- en regelgeving, sectorspecifieke eisen en het beleid en de procedures van de entiteit. | VV, V |
| *Gerelateerde kernelementen van de AVG:*   * Beveiliging van de verwerking * Privacyprincipes | | |

|  |  |  |
| --- | --- | --- |
| Juridische beoordeling van wijzigingen in wet- en regelgeving en/of bedrijfsvereisten (LRC)  *Beheersingsdoelstelling:*  De entiteit houdt voldoende rekening met privacyrisico's die voortkomen uit veranderingen binnen de entiteit (structuur en strategie) en wet- en regelgeving. | | |
| *Fase informatielevenscyclusmanagement:* **Management** | | |
| *Beheersingsmaatregelen:* | |  |
| LRC01 | De entiteit richt een proces in om het effect op de privacyvereisten te monitoren, beoordelen en te behandelen van wijzigingen in:   1. wet- en regelgeving; 2. sectorspecifieke eisen, best practices en richtlijnen; 3. overeenkomsten, waaronder Service Level Agreements met derden (wijzigingen van de bepalingen inzake privacy en beveiliging in overeenkomsten worden op adequate wijze geëvalueerd en goedgekeurd voordat zij worden uitgevoerd); 4. bedrijfsactiviteiten en processen; 5. personen die worden belast met de verantwoordelijkheid voor privacy en beveiliging; 6. technologie (voordat deze wordt geïmplementeerd). | VV, V |
| *Gerelateerde kernelementen van de AVG:*   * Gegevensbeschermingseffectbeoordeling * Rechtmatigheid van de verwerking | | |

Informeren

|  |  |  |
| --- | --- | --- |
| Privacyverklaring (PST)  *Beheersingsdoelstelling:*  De entiteit informeert betrokkenen op transparante wijze over het beleid, de voorwaarden en activiteiten met betrekking tot het verzamelen, gebruiken, bewaren, verstrekken en verwijderen van persoonsgegevens. | | |
| *Fase informatielevenscyclusmanagement:* **Informeren** | | |
| *Beheersingsmaatregelen:* | |  |
| PST01 | In de privacyverklaring van de entiteit staat:   1. welke persoonsgegevens worden verzameld, waar deze  informatie vandaan komt, de doeleinden voor de verzameling en de betreffende rechtsgronden voor de verwerking; 2. wat de gevolgen zijn, voor zover daar sprake van is, als de  betrokkene de gevraagde gegevens niet verstrekt; 3. informatie over verdere verwerking (indien van toepassing); 4. informatie over de rechten van betrokkenen en de wijze waarop zij die rechten kunnen uitoefenen (zie ook URE, DAR, DCR, DDR, DPR). | VV |
| PST02 | De privacyverklaring:   1. is gemakkelijk toegankelijk en beschikbaar voor betrokkenen  op het moment dat voor het eerst persoonsgegevens van de  betrokkene worden verzameld; 2. wordt tijdig beschikbaar gesteld (ten tijde van of voorafgaand  aan het moment dat persoonsgegevens worden verzameld, of zo spoedig mogelijk erna) zodat de betrokkene de keuze heeft om de persoonsgegevens wel of niet te verstrekken; 3. is duidelijk van een datum voorzien, zodat betrokkenen kunnen zien of de verklaring is aangepast sinds zij deze hebben gelezen of sinds de laatste keer dat zij persoonsgegevens aan de entiteit hebben verstrekt; 4. is eenvoudig te begrijpen en leesbaar. | VV |
| *Gerelateerde kernelementen van de AVG:*   * Rechten van de betrokkene * Verantwoordelijkheden van verwerkingsverantwoordelijke en verwerker * Privacyprincipes | | |

Keuze en toestemming

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Toestemmingsraamwerk (CFR)  *Beheersingsdoelstelling:*  De entiteit verkrijgt indien vereist of noodzakelijk toestemming van de betrokkene om persoonsgegevens te verwerken. | | | | | |
| *Fase informatielevenscyclusmanagement:* **Keuze en toestemming** | | | | | |
| *Beheersingsmaatregelen:* | | | | *Bevindingen/ toetsing:* | |
| CFR01 | | In de privacyverklaring beschrijft de entiteit op duidelijke en beknopte wijze:   1. welke keuzes de betrokkene heeft met betrekking tot de verzameling, het gebruik, en de verstrekking van persoonsgegevens; 2. wat de betrokkene moet doen om deze keuzes te maken (zoals het aanvinken van een vakje om aan te geven dat hij/zij geen marketingmateriaal wenst te ontvangen); 3. de mogelijkheid om de contactvoorkeuren aan te passen en hoe de betrokkene dit doet; 4. wat de gevolgen zijn als de persoonsgegevens die nodig zijn voor een transactie of dienst niet worden verstrekt; 5. wat de gevolgen zijn als de persoon weigert persoonsgegevens te verstrekken (transacties kunnen bijvoorbeeld mogelijk niet worden verwerkt); 6. wat de gevolgen zijn van het niet verlenen of intrekken van toe-stemming (als de persoon bijvoorbeeld geen informatie wenst te ontvangen over producten en diensten, wordt hij of zij mogelijk niet op de hoogte gebracht van acties). | | VV | |
| CFR02 | | Wanneer de verwerking is gebaseerd op de grondslag toestemming:   1. verkrijgt en documenteert de entiteit tijdig de toestemming van de betrokkene (ten tijde van of voorafgaand aan het moment dat de persoonsgegevens worden verzameld, of kort erna); 2. legt de entiteit de voorkeuren van de betrokkene vast (schriftelijk of elektronisch); 3. documenteert de entiteit wijzigingen in de contactvoorkeuren en verwerkt deze; 4. zorgt de entiteit dat de voorkeuren van de betrokkene tijdig worden verwerkt; 5. bewaart de entiteit de informatie om aan kunnen te tonen dat de betrokkene toestemming heeft verleend. | | VV | |
| CFR03 | | De entiteit verzamelt of verwerkt geen bijzondere categorieën van persoonsgegevens, tenzij de entiteit hiervoor een wettelijke grondslag heeft.  Wanneer de uitdrukkelijke toestemming van de betrokkene de wettelijke grondslag is voor de verwerking van bijzondere categorieën van  persoonsgegevens, heeft de betrokkene door middel van een duidelijke actieve handeling ingestemd met het gebruik of de verstrekking van  bijzondere categorieën van persoonsgegevens. De entiteit verkrijgt de uitdrukkelijke toestemming rechtstreeks van de betrokkene en documenteert/bewaart het bewijs dat deze toestemming is verleend, bijvoorbeeld door de persoon te vragen een vakje aan te vinken of een formulier te ondertekenen. | | VV | |
| CFR04 | | Wanneer de verwerking van persoonsgegevens berust op toestemming, faciliteert de entiteit de uitoefening van het recht van de betrokkene om zijn toestemming te allen tijde in te trekken. | | VV | |
| *Gerelateerde kernelementen van de AVG:*   * Rechtmatigheid van de verwerking * Voorwaarden voor toestemming * Rechten van de betrokkene | | | | | |

Verzamelen

|  |  |  |
| --- | --- | --- |
| Minimale gegevensverwerking (DMI)  *Beheersingsdoelstelling:*  De persoonsgegevens zijn toereikend, ter zake dienend en beperkt tot wat noodzakelijk is voor de gerechtvaardigde doeleinden waarvoor zij worden verwerkt. | | |
| *Fase informatielevenscyclusmanagement:* **Verzamelen** | | |
| *Beheersingsmaatregelen:* | |  |
| DMI01 | De entiteit richt een proces en procedures in om:   1. te bepalen welke persoonsgegevens noodzakelijk zijn voor het doel van de verwerking en welke persoonsgegevens optioneel zijn; 2. de verwerking van persoonsgegevens te beperken tot het voor het doel noodzakelijke minimum; 3. periodiek na te gaan of de verwerking van persoonsgegevens nog noodzakelijk is voor de producten en/of diensten van de entiteit. | VV |
| DMI02 | In het privacybeleid van de entiteit is opgenomen dat minimale gegevensverwerking een privacyprincipe is (zie PPO). | VV |
| *Gerelateerde kernelementen van de AVG:*   * Privacyprincipes * Gegevensbescherming door ontwerp / door standaardinstellingen | | |

Gebruiken, opslaan en verwijderen

|  |  |  |
| --- | --- | --- |
| Doelbinding (ULI)  *Beheersingsdoelstelling:*  Persoonsgegevens worden niet verstrekt, beschikbaar gesteld of anderszins voor andere doeleinden gebruikt dan die zijn geformuleerd in de privacyverklaring van de entiteit, tenzij:   * de betrokkene toestemming verleent; of * dit wettelijk vereist is. | | |
| *Fase informatielevenscyclusmanagement:* **Gebruiken, opslaan en verwijderen** | | |
| *Beheersingsmaatregelen:* | |  |
| ULI01 | De entiteit richt een proces en procedures in om:   1. de verstrekking en het gebruik van persoonsgegevens te beperken tot de gerechtvaardigde doeleinden die worden genoemd in het privacybeleid en de privacyverklaring van de entiteit; 2. bij voortduring te waarborgen dat de verstrekking en het gebruik van persoonsgegevens overeenkomstig de toestemming van de betrokkene en de betreffende wet- en regelgeving is. | VV |
| ULI02 | In het privacybeleid van de entiteit is opgenomen dat doelbinding een privacyprincipe is (zie PPO). | VV |
| *Gerelateerde kernelementen van de AVG:*   * Privacyprincipes * Gegevensbescherming door ontwerp / door standaardinstellingen | | |

|  |  |  |
| --- | --- | --- |
| Privacyarchitectuur (Gegevensbescherming door ontwerp en door standaardinstellingen) (PBD)  *Beheersingsdoelstelling:*  De entiteit neemt bij het ontwikkelen en wijzigen van producten, diensten, bedrijfssystemen of processen het solide privacybeleid, de privacyprincipes en/of de van toepassing zijnde wet- en regelgeving in acht. | | |
| *Fase informatielevenscyclusmanagement:* **Gebruiken, opslaan en verwijderen** | | |
| *Beheersingsmaatregelen:* | |  |
| PBD01 | Bij de ontwikkeling, het ontwerp, selectie en het gebruik van toepassin-gen, diensten en producten waarbij persoonsgegevens worden verwerkt, houdt de entiteit zo vroeg mogelijk in het ontwerpproces rekening met de privacyprincipes en privacyrisico's. Het risico op strijdigheid tussen het ontwerp en de rechten en vrijheden van betrokkenen (en het privacybeleid van de entiteit) is geïdentificeerd en aangepakt.  Wanneer de entiteit diensten van derden bij deze activiteiten betrekt, verplicht de entiteit deze partijen om dezelfde risicomanagementactiviteiten ten aanzien van privacy te hanteren. | VV |
| PBD02 | De beoordeling van privacyrisico's is een inherent en gedocumenteerd onderdeel van de projectmethodiek en/of het ontwikkelingsproces van de entiteit. | VV |
| PBD03 | Wanneer systemen, diensten en producten waarbij persoonsgegevens worden verwerkt privacy-gerelateerde opties bieden, zijn deze standaard ingesteld op de meest beperkende optie met betrekking tot privacy. | VV |
| *Gerelateerde kernelementen van de AVG:*   * Gegevensbescherming door ontwerp / door standaardinstellingen * Privacyprincipes | | |

|  |  |  |
| --- | --- | --- |
| Bewaren van gegevens (DRE)  *Beheersingsdoelstelling:*  Persoonsgegevens worden niet langer bewaard dan noodzakelijk, dan wettelijk is toegestaan of dan noodzakelijk is voor de doeleinden waarvoor zij werden verzameld. | | |
| *Fase informatielevenscyclusmanagement:* **Gebruiken, opslaan en verwijderen** | | |
| *Beheersingsmaatregelen:* | |  |
| DRE01 | De entiteit:   1. documenteert het bewaarbeleid en de verwijderingsprocedures ten aanzien van persoonsgegevens; 2. zorgt dat persoonsgegevens niet langer worden bewaard dan de vastgestelde bewaartermijn, tenzij er sprake is van een gerechtvaardigde reden of wettelijke verplichting. 3. documenteert voor elke verwerking van persoonsgegevens de  betreffende bewaartermijn; 4. informeert betrokkenen in de privacyverklaring over het beleid ten aanzien van bewaartermijnen; 5. slaat gearchiveerde kopieën en back-ups op, bewaart en  verwijdert deze overeenkomstig het bewaarbeleid; 6. instrueert verwerkers over bewaartermijnen. | VV |
| DRE02 | Bij het vaststellen van bewaarprocedures worden wettelijke en contractuele bewaartermijnen in acht genomen; deze wijken mogelijk af van de normale beleidsregels. | VV |
| *Gerelateerde kernelementen van de AVG:*   * Privacyprincipes * Verantwoordelijkheden van verwerkingsverantwoordelijke en verwerker | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Verwijdering, vernietiging en anonimisatie (DDA)  *Beheersingsdoelstelling:*  Persoonsgegevens worden indien nodig geanonimiseerd en/of verwijderd binnen de entiteit. De identiteit van personen kan niet worden herleid en persoonsgegevens zijn niet meer beschikbaar nadat de bewaartermijn is verstreken. | | | | |
| *Fase informatielevenscyclusmanagement:* **Gebruiken, opslaan en verwijderen** | | | | |
| *Beheersingsmaatregelen:* | | |  | |
| DDA01 | | De entiteit heeft een gedocumenteerde procedure ingericht om te waarborgen dat:   1. het wissen en vernietigen van persoonsgegevens geschiedt  conform het bewaarbeleid, ongeacht de vorm waarin deze zijn opgeslagen (zoals elektronisch, op optische media, of op papier); 2. de verwijdering van originele, gearchiveerde gegevens, back-ups en persoonlijke kopieën conform het vernietigingsbeleid plaatsvindt; 3. de verwijdering van persoonsgegevens op een adequate wijze wordt vastgelegd.   De entiteit zorgt er daarnaast voor dat:   1. persoonsgegevens worden gelokaliseerd en verwijderd of teruggebracht, voor zover dit technisch mogelijk is. 2. persoonsgegevens die niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of gegevens die op grond van wet- en regelgeving moeten worden verwijderd, op regelmatige en systematische basis worden vernietigd, gewist of geanonimiseerd. | VV | |
| DDA02 | | Bij het vaststellen van procedures voor verwijdering, vernietiging en vermindering van persoonsgegevens worden contractbepalingen in acht genomen indien deze afwijken van de normale beleidsregels. | VV | |
| *Gerelateerde kernelementen van de AVG:*   * Privacyprincipes * Verantwoordelijkheden van verwerkingsverantwoordelijke en verwerker * Beveiliging van de verwerking * Gegevensbescherming door ontwerp / door standaardinstellingen | | | | |

|  |  |  |
| --- | --- | --- |
| Gebruik en beperking (URE)  *Beheersingsdoelstelling:*  Persoonsgegevens worden niet verwerkt als de betrokkene een beperking van de verwerking heeft verkregen of wanneer er sprake is van specifieke juridische restricties door lokale autoriteiten. Bezwaren van de betrokkene tegen de verwerking van persoonsgegevens worden op een adequate wijze afgehandeld. | | |
| *Fase informatielevenscyclusmanagement:* **Gebruiken, opslaan en verwijderen** | | |
| *Beheersingsmaatregelen:* | |  |
| ~~URE01~~ | *Samengevoegd met PST01.* |  |
| URE02 | De entiteit heeft een proces ingericht om adequaat te handelen wanneer betrokkenen hun recht op beperking van of bezwaar tegen de verwerking uitoefenen. | VV |
| URE03 | De entiteit heeft vastgesteld of lidstaatrechtelijke bepalingen de verwerking van persoonsgegevens beperken (bijvoorbeeld ter bescherming van de nationale of openbare veiligheid) en kan aantonen dat deze beperkingen worden gehandhaafd. | VV |
| *Gerelateerde kernelementen van de AVG:*   * Privacyprincipes * Rechtmatigheid van de verwerking * Rechten van de betrokkene * Doorgiften van persoonsgegevens aan derde landen of internationale organisaties | | |

Inzage en kwaliteit van gegevens

|  |  |  |
| --- | --- | --- |
| Verzoek tot inzage (DAR)  *Beheersingsdoelstelling:*  Een inzageverzoek van de betrokkene wordt op de juiste wijze afgehandeld en betrokkenen kunnen nagaan welke persoonsgegevens van hen worden verwerkt en op welke manier. | | |
| *Fase informatielevenscyclusmanagement:* **Inzage en kwaliteit van gegevens** | | |
| *Beheersingsmaatregelen:* | |  |
| DAR01 | De entiteit heeft procedures ingericht om adequaat te reageren op inzageverzoeken van betrokkenen. Indien de betrokkene het recht op inzage uitoefent, verstrekt de entiteit aan de betrokkene informatie over de aard van de verwerkte persoonsgegevens en de kenmerken van de verwerking (bijv. het doel, de ontvangers, de bewaartermijnen, het bestaan van geautomatiseerde besluitvorming). | VV |
| ~~DAR02~~ | *Samengevoegd met PST01*. |  |
| DAR03 | De entiteit heeft een proces ingericht om tijdig een kopie van de verwerkte persoonsgegevens aan de betrokkene te verstrekken in een gangbare elektronische vorm. | VV |
| DAR04 | De entiteit verifieert de identiteit van de betrokkene alvorens informatie te verstrekken. | VV |
| *Gerelateerde kernelementen van de AVG:*   * Beveiliging van de verwerking * Gegevensbescherming door ontwerp / door standaardinstellingen * Rechten van de betrokkene | | |

|  |  |  |
| --- | --- | --- |
| Verzoek tot rectificatie (DCR)  *Beheersingsdoelstelling:*  Een rectificatieverzoek van de betrokkene wordt op de juiste wijze afgehandeld. Betrokkenen kunnen bepalen of hun persoonsgegevens correct/up-to-date zijn en zij kunnen deze corrigeren. | | |
| *Fase informatielevenscyclusmanagement:* **Inzage en kwaliteit van gegevens** | | |
| *Beheersingsmaatregelen:* | |  |
| DCR01 | De entiteit heeft procedures ingericht om adequaat te reageren op rectificatieverzoeken van betrokkenen. Indien de betrokkene het recht op rectificatie uitoefent, corrigeert de entiteit de persoonsgegevens onverwijld. | VV |
| ~~DCR02~~ | *Samengevoegd met PST01.* |  |
| DCR03 | De entiteit verifieert de identiteit van de betrokkene alvorens het verzoek in te willigen. | VV |
| DCR04 | De entiteit stelt partijen waar de persoonsgegevens aan zijn verstrekt op de hoogte van de wijzigingen. | VV |
| *Gerelateerde kernelementen van de AVG:*   * Rechten van de betrokkene | | |

|  |  |  |
| --- | --- | --- |
| Verzoek tot wissen (DDR)  *Beheersingsdoelstelling:*  Een verzoek tot het wissen van persoonsgegevens van de betrokkene wordt op de juiste wijze afgehandeld en betrokkenen kunnen bepalen welke persoonsgegevens zij willen laten wissen, mits aan de geldende criteria wordt voldaan. | | |
| *Fase informatielevenscyclusmanagement:* **Inzage en kwaliteit van gegevens** | | |
| *Beheersingsmaatregelen:* | |  |
| DDR01 | De entiteit heeft procedures ingericht om adequaat te reageren op een verzoek tot het wissen van persoonsgegevens (‘recht op vergetelheid’). Indien de betrokkene het recht op gegevenswissing uitoefent, toetst de entiteit de gronden van het verzoek aan de geldende criteria (bijv. de verwerking berust op toestemming, de verwerking is onrechtmatig, het doel is niet langer geldig, wettelijke vereisten voor bewaren). Als de grond gerechtvaardigd is, wist de entiteit de persoonsgegevens onverwijld. | VV |
| DDR02 | Indien van toepassing stelt de entiteit andere verwerkingsverantwoordelijken waar de persoonsgegevens aan zijn verstrekt op de hoogte van het verzoek van de betrokkene om persoonsgegevens te laten wissen. Indien de persoonsgegevens worden verwerkt door een verwerker, instrueert de entiteit de verwerker de gegevens te wissen. | VV |
| ~~DDR03~~ | *Samengevoegd met PST01.* |  |
| DDR04 | De entiteit verifieert de identiteit van de betrokkene alvorens het verzoek in te willigen. | VV |
| *Gerelateerde kernelementen van de AVG:*   * Rechten van de betrokkene | | |

|  |  |  |
| --- | --- | --- |
| Verzoek tot overdracht (DPR)  *Beheersingsdoelstelling:*  Een verzoek tot overdracht van persoonsgegevens van de betrokkene wordt op de juiste wijze afgehandeld en betrokkenen kunnen hun persoonsgegevens laten overdragen aan een andere entiteit, mits aan de geldende criteria wordt voldaan. | | |
| *Fase informatielevenscyclusmanagement:* **Inzage en kwaliteit van gegevens** | | |
| *Beheersingsmaatregelen:* | |  |
| DPR01 | De entiteit heeft procedures ingericht om adequaat te reageren op een verzoek tot overdracht van persoonsgegevens. Indien de betrokkene het recht op overdracht uitoefent, toetst de entiteit de gronden van het verzoek aan de geldende criteria (bijv. de verwerking berust op toestemming, de verwerking wordt via geautomatiseerde procedés verricht). Als de grond gerechtvaardigd is, draagt de entiteit de persoonsgegevens zonder onnodige vertraging over. | VV |
| DPR02 | Als het technisch gezien mogelijk is, draagt de entiteit de persoonsgegevens rechtstreeks over aan de door de betrokkene aangewezen entiteit (verwerkingsverantwoordelijke). | VV |
| ~~DPR03~~ | *Samengevoegd met PST01.* |  |
| DPR04 | De entiteit verifieert de identiteit van de betrokkene alvorens het verzoek in te willigen. | VV |
| *Gerelateerde kernelementen van de AVG:*   * Rechten van de betrokkene * Recht op overdraagbaarheid van gegevens | | |

|  |  |  |
| --- | --- | --- |
| Juistheid en volledigheid van gegevens (ACD)  *Beheersingsdoelstelling:*  Vastgelegde procedures voor het valideren, aanpassen en bijwerken van persoonsgegevens waarborgen de juistheid en volledigheid van persoonsgegevens | | |
| *Fase informatielevenscyclusmanagement:* **Inzage en kwaliteit van gegevens** | | |
| *Beheersingsmaatregelen:* | |  |
| ACD01 | De entiteit heeft procedures opgesteld om:   1. persoonsgegevens aan te passen en te valideren wanneer deze worden verzameld, gecreëerd, bijgehouden en bijgewerkt; 2. de datum vast te leggen waarop de persoonsgegevens zijn verkregen of bijgewerkt; 3. te specificeren wanneer de persoonsgegevens niet meer geldig zijn; 4. te specificeren wanneer en hoe de persoonsgegevens dienen te worden bijgewerkt en wat de bron voor de bijwerking is (bijvoorbeeld een jaarlijkse herbevestiging van de beschikbare informatie en methoden om persoonsgegevens proactief te laten bijwerken door betrokkenen); 5. de juistheid en volledigheid te verifiëren van persoonsgegevens die zijn verkregen van de betrokkene of van derden, of die zijn verstrekt aan derden; 6. te waarborgen dat de verwerkte persoonsgegevens juist en volledig genoeg zijn om beslissingen op te baseren. | VV |
| ACD02 | De entiteit voert periodiek beoordelingen uit om de juistheid van persoonsgegevens te controleren en deze zo nodig te corrigeren, teneinde het betreffende doel te verwezenlijken. | VV |
| *Gerelateerde kernelementen van de AVG:*   * Beveiliging van de verwerking | | |

Verstrekken

|  |  |  |
| --- | --- | --- |
| Verstrekking aan derden en registratie (TPD)  *Beheersingsdoelstelling:*  Persoonsgegevens worden niet aan derden verstrekt zonder wettelijke basis of voor andere doeleinden dan waarover de betrokkene is geïnformeerd. | | |
| *Fase informatielevenscyclusmanagement:* **Verstrekken** | | |
| *Beheersingsmaatregelen:* | |  |
| TPD01 | De entiteit heeft procedures ingericht om:   1. te voorkomen dat persoonsgegevens aan derden worden verstrekt, terwijl de wettelijke basis daarvoor ontbreekt en/of de betrokkene daarover niet is geïnformeerd; 2. te documenteren wat de aard van de persoonsgegevens is die aan derden worden verstrekt en in welke mate deze worden verstrekt; 3. te monitoren of de verstrekking aan derden nog steeds in overeenstemming is met het privacybeleid en de privacyprocedures van de entiteit, of uitdrukkelijk is toegestaan of verplicht is op grond van wet- of regelgeving; 4. te documenteren of persoonsgegevens aan derden worden verstrekt om juridische redenen; 5. betrokkenen te informeren en hun toestemming te verkrijgen om persoonsgegevens te verstrekken aan derden voor doeleinden die niet in de privacyverklaring staan; 6. erop toe te zien dat persoonsgegevens alleen aan derden worden verstrekt voor de doeleinden in de privacyverklaring. | VV |
| *Gerelateerde kernelementen van de AVG:*   * Beveiliging van de verwerking * Rechtmatigheid van de verwerking | | |

|  |  |  |
| --- | --- | --- |
| Overeenkomsten met derden (TPA)  *Beheersingsdoelstelling:*  Bij de verwerving van oplossingen en diensten (gerelateerd aan persoonsgegevens) van derden wordt voldoende aandacht besteed aan privacyoverwegingen en -vereisten, waardoor op de juiste wijze met persoonsgegevens wordt omgegaan en deze worden beschermd. | | |
| *Fase informatielevenscyclusmanagement:* **Verstrekken** | | |
| *Beheersingsmaatregelen:* | |  |
| TPA01 | (a) Indien de entiteit oplossingen van derden/leveranciers verwerft of processen aan dienstverleners uitbesteedt en de verwerking van persoonsgegevens (gedeeltelijk) extern plaatsvindt, gaat de entiteit formele overeenkomsten aan die de derden ertoe verplichten de nodige zorgvuldigheid te betrachten en een beschermingsniveau te waarborgen dat gelijk is aan dat van de entiteit. Op deze wijze beperkt de entiteit het gebruik van persoonsgegevens door derden tot de door de entiteit vastgestelde doeleinden.  (b) De entiteit zorgt dat het (verder) uitbesteden van de verwerking van persoonsgegevens slechts plaatsvindt na goedkeuring daarvan door de verwerkingsverantwoordelijke. Indien die toestemming wordt verleend, gaat de entiteit formele overeenkomsten aan die de derde partij ertoe verplichten de nodige zorgvuldigheid te betrachten en een beschermingsniveau te waarborgen dat gelijk is aan dat van de entiteit. | VV  V |
| TPA02 | De entiteit zorgt dat in de overeenkomsten eveneens de volgende verplichtingen voor de andere partij zijn opgenomen:   1. vertrouwelijkheids- en geheimhouding; 2. beveiligingsvereisten; 3. medewerking bij het behandelen van verzoeken van betrokkenen en de uitoefening van rechten van de betrokkenen; 4. informatieverstrekking (bijv. in het geval van geplande uitbesteding); 5. informatieverstrekking en medewerking bij inbreuken in verband met persoonsgegevens; 6. bewaartermijnen en verwijdering van gegevens; 7. geen verdere uitbesteding zonder toestemming van de entiteit; 8. aansprakelijkheid en vrijwaring. | VV, V |
| TPA03 | De entiteit evalueert de prestaties en de naleving van de verplichtingen door derden aan de hand van een of meerdere methoden (in oplopende volgorde van zekerheid en afhankelijk van het risicoprofiel van de derde partij):   1. de derde partij vult een vragenlijst in over de manier van werken; 2. de derde partij beoordeelt zelf of de werkwijzen voldoen aan de vereisten van de entiteit op basis van interne auditrapporten of andere procedures; 3. de entiteit voert periodiek een evaluatie op locatie uit bij de derde partij; 4. de entiteit laat een audit of assurance assessment uitvoeren door een onafhankelijke auditor. | VV, V |
| *Gerelateerde kernelementen van de AVG:*   * Verantwoordelijkheden van verwerkingsverantwoordelijke en verwerker * Beveiliging van de verwerking | | |

|  |  |  |
| --- | --- | --- |
| Doorgifte van persoonsgegevens (DTR) | | |
| *Beheersingsdoelstelling:*  Persoonsgegevens worden niet doorgegeven (d.w.z. verplaatst, weergegeven of geprint op een andere locatie) aan landen die geen toereikend rechtskader ten aanzien van privacy hebben. | | |
| *Fase informatielevenscyclusmanagement:* **Verstrekken** | | |
| *Beheersingsmaatregelen:* | |  |
| DTR01 | De entiteit heeft alle gevallen in kaart gebracht waarin persoonsgegevens waar zij de verantwoordelijkheid voor draagt worden doorgegeven aan en verwerkt in derde landen die mogelijk de privacy van betrokkenen niet voldoende waarborgen. | VV, V |
| DTR02 | De entiteit geeft alleen persoonsgegevens door aan derde landen (a) waarvoor de Europese Commissie een adequaatheidsbesluit heeft  genomen, of (b) die een set passende waarborgen hebben getroffen (bijv. bindende bedrijfsvoorschriften of standaardbepalingen inzake gegevensbescherming). | VV, V |
| *Gerelateerde kernelementen van de AVG:*   * Doorgiften van persoonsgegevens aan derde landen of internationale organisaties | | |

Gegevensbeveiliging

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Programma informatiebeveiliging (ISP)  *Beheersingsdoelstelling:*  Persoonsgegevens worden adequaat beschermd tegen onopzettelijke fouten of verlies, of kwaadwillige handelingen zoals hacken, diefstal, ongeautoriseerde verstrekking of verlies. | | | | | |
| *Fase informatielevenscyclusmanagement:* **Gegevensbeveiliging** | | | | | |
| *Beheersingsmaatregelen:* | | | |  | |
| ISP01 | | De entiteit heeft passende technische en organisatorische maatregelen  genomen om de beveiliging van persoonsgegevens te waarborgen. De beveiliging omvat de vertrouwelijkheid, integriteit en beschikbaarheid van persoonsgegevens. Zie ook IAM, STR, ENC, LOG. | | VV, V | |
| ISP02 | | De beveiliging van persoonsgegevens komt uitdrukkelijk aan de orde in het beleid van de entiteit voor informatiebeveiliging en het managementsysteem voor informatiebeveiliging. | | VV, V | |
| ISP03 | | In hoeverre de beveiligingsmaatregelen met betrekking tot persoonsgegevens adequaat zijn, wordt bepaald door middel van periodieke risicobeoordelingen waaraan alle relevante belanghebbenden deelnemen en waarbij zowel naar de huidige als de toekomstige verwerkingsactiviteiten wordt gekeken. | | VV, V | |
| ISP04 | | De entiteit heeft een gedocumenteerd beleid ten aanzien van versleuteling en pseudonimisering van persoonsgegevens en verifieert systematisch dat het beleid wordt nageleefd (zie ook ENC). | | VV, V | |
| ISP05 | | De entiteit toetst, beoordeelt en evalueert op regelmatige basis de effectiviteit van de technische en organisatorische beveiligingsmaatregelen om een adequaat beveiligingsniveau te waarborgen en verbeteringen te identificeren en door te voeren. | | VV, V | |
| ISP06 | | De entiteit stelt zich actief op tegenover het gebruik van een gedragscode (van branche- en beroepsverenigingen of sectororganisaties) en/of certificeringen om aan te tonen dat de entiteit een passend beschermingsniveau waarborgt. | | VV, V | |
| ISP07 | | Het beveiligingsprogramma van de entiteit voorkomt dat personen toegang hebben tot persoonsgegevens in computers, media en op papier die niet  meer actief door de organisatie worden gebruikt (zoals computers, media en informatie op papier die zijn opgeslagen, verkocht of op andere wijze zijn  verwijderd). | | VV, V | |
| *Gerelateerde kernelementen van de AVG:*   * Beveiliging van de verwerking | | | | | |
| Identiteit en toegangsbeheer (IAM)  *Beheersingsdoelstelling:*  Toegangsrechten worden adequaat toegekend, gewijzigd en ingetrokken. Dit verkleint de kans opop ongeautoriseerde toegang tot en onjuiste verwerking van persoonsgegevens, of inbreuk in verband met persoonsgegevens door interne medewerkers, derden of hackers.. | | | | | |
| *Fase informatielevenscyclusmanagement:* **Gegevensbeveiliging** | | | | | |
| *Beheersingsmaatregelen:* | | | |  | |
| IAM01 | | De entiteit heeft systemen en procedures ingericht om:   1. vast te stellen in hoeverre en op welke wijze gebruikers toegang krijgen tot persoonsgegevens. Dit is gebaseerd op de gevoeligheid van de gegevens en de gerechtvaardigde zakelijke doeleinden van de gebruikers; 2. gebruikers te identificeren en te authenticeren (bijvoorbeeld door middel van een gebruikersnaam en wachtwoord, certificaat, extern token of biometrische gegevens) voordat toegang wordt verleend tot systemen die persoonsgegevens verwerken; 3. strengere beveiligingsmaatregelen in te stellen voor toegang op afstand, zoals extra of dynamische wachtwoorden, callback-procedures, digitale certificaten, beveiligde ID-kaarten, virtual private network (VPN), of adequaat geconfigureerde firewalls; 4. toegangsdetectie en monitoringssystemen te implementeren. | | VV, V | |
| *Gerelateerde kernelementen van de AVG:*   * Beveiliging van de verwerking | | | | | |

|  |  |  |
| --- | --- | --- |
| Veilige gegevensoverdracht (STR)  *Beheersingsdoelstelling:*  Door beperkte toegang tot persoonsgegevens tijdens verzending wordt op adequate wijze ongeautoriseerde verstrekking, inbreuk, wijziging of verwijdering van persoonsgegevens voorkomen. | | |
| *Fase informatielevenscyclusmanagement:* **Gegevensbeveiliging** | | |
| *Beheersingsmaatregelen:* | |  |
| STR01 | De entiteit heeft systemen en procedures ingericht om:   1. het minimumniveau van beveiliging vast te stellen voor verzending van persoonsgegevens; 2. bij het doorgeven en ontvangen van persoonsgegevens versleutelingstechnologie toe te passen die de standaard is in de sector; 3. externe netwerkverbindingen te beoordelen en goed te keuren; 4. persoonsgegevens te beschermen in zowel gedrukte als elektronische vorm, verstuurd per post, koerier of andere fysieke methode; 5. via draadloze netwerken verzamelde en verzonden persoonsgegevens te versleutelen en draadloze netwerken te beschermen tegen ongeautoriseerde toegang. | VV, V |
| *Gerelateerde kernelementen van de AVG:*   * Beveiliging van de verwerking * Inbreuk in verband met persoonsgegevens | | |

|  |  |  |
| --- | --- | --- |
| Versleuteling en eindpuntbeveiliging (ENC)  *Beheersingsdoelstelling:*  Inbreuk in verband met persoonsgegevens (onopzettelijk verlies of kwaadwillige handelingen zoals diefstal, ongeautoriseerde verstrekking of verlies) wordt voorkomen door middel van versleuteling. | | |
| *Fase informatielevenscyclusmanagement:* **Gegevensbeveiliging** | | |
| *Beheersingsmaatregelen:* | |  |
| ENC01 | Beleidsregels en procedures verbieden de opslag van persoonsgegevens op draagbare media of apparaten, tenzij er sprake is van zakelijke noodzaak en de opslag is goedgekeurd door het management. | VV, V |
| ENC02 | De entiteit heeft beleid, systemen en procedures opgesteld om persoonsgegevens te beschermen die toegankelijk zijn via of zijn opgeslagen op de volgende apparaten:   1. laptops, pda’s, smartphones en vergelijkbare apparaten; 2. computers en andere apparaten die medewerkers gebruiken als zij bijvoorbeeld onderweg zijn of vanuit huis werken; 3. USB-sticks, cd’s, dvd’s, magneetband en andere draagbare media.   Dergelijke informatie wordt versleuteld, beveiligd met een wachtwoord en fysiek beschermd, en hierop is het toegangs-, bewaar- en vernietigingsbeleid van de entiteit van toepassing. | VV, V |
| ENC03 | De entiteit heeft procedures en systemen voor het creëren, verplaatsen, opslaan en verwijderen van media met persoonsgegevens die zijn gebruikt voor back-ups en herstel. | VV, V |
| ENC04 | De entiteit heeft procedures voor het rapporteren van mogelijk misbruik van media met persoonsgegevens (zie ook PIA). Wanneer het dienstverband van medewerkers of overeenkomsten met derden worden beëindigd, zijn er procedures voor het terughalen en vernietigen van draagbare media en apparaten die gebruikt zijn om toegang te verkrijgen tot persoonsgegevens of deze op te slaan. Dit geldt eveneens voor geprinte informatie en andere bestaande kopieën. | VV, V |
| *Gerelateerde kernelementen van de AVG:*   * Beveiliging van de verwerking * Inbreuk in verband met persoonsgegevens | | |

|  |  |  |
| --- | --- | --- |
| Registreren van toegang (LOG)  *Beheersingsdoelstelling:*  Toegang of toegangspogingen tot persoonsgegevens door medewerkers en derden worden geregistreerd en onderzocht om (pogingen tot) inbreuk op de beveiliging van persoonsgegevens te detecteren en te voorkomen. | | |
| *Fase informatielevenscyclusmanagement:* **Gegevensbeveiliging** | | |
| *Beheersingsmaatregelen:* | |  |
| LOG01 | De entiteit heeft systemen en procedures ingericht om:   1. de logische en fysieke toegang tot persoonsgegevens te beheren, inclusief hardcopy's, archiefkopieën en back-upkopieën; 2. de toegang tot systemen met persoonsgegevens (of pogingen hiertoe) te registreren en te monitoren. De logbestanden bevat voldoende details en wordt lang genoeg bewaard om de gegevens te kunnen analyseren en onderzoeken; 3. het ongeautoriseerd of onopzettelijk vernietigen of verliezen van persoonsgegevens te voorkomen; 4. inbreuken in verband met persoonsgegevens en pogingen om ongeautoriseerde toegang te verkrijgen te onderzoeken. | VV, V |
| *Gerelateerde kernelementen van de AVG:*   * Beveiliging van de verwerking * Inbreuk in verband met persoonsgegevens | | |

Monitoren en handhaven

|  |  |  |
| --- | --- | --- |
| Beoordeling van naleving privacywetgeving (REV)  *Beheersingsdoelstelling:*  Adequaat toezicht op de interne organisatie en derden waarborgt dat de entiteit voldoet aan de wet- en regelgeving met betrekking tot privacy en vermindert het risico op inbreuk in verband met persoonsgegevens of verlies hiervan.. | | |
| *Fase informatielevenscyclusmanagement:* **Monitoren en handhaven** | | |
| *Beheersingsmaatregelen:* | |  |
| REV01 | De entiteit heeft systemen en procedures ingericht om:   1. jaarlijks de naleving te beoordelen van privacybeleid en  -procedures, verplichtingen en geldende wet- en regelgeving, Service Level Agreements, door de entiteit opgestelde normen en andere overeenkomsten; 2. periodiek beoordelingen te documenteren, zoals, interne auditplannen, auditrapporten, compliance checklists en aftekeningen (‘sign-offs’) van het management; 3. de resultaten van de conformiteitsbeoordeling en aanbevelingen voor verbetering aan het management te rapporteren, en een verbeterplan te implementeren; 4. de oplossing van problemen en de kwetsbaarheden die naar voren komen in de conformiteitsbeoordeling te monitoren, om te waarborgen dat tijdig passende corrigerende maatregelen worden genomen (waaronder herziening van het privacybeleid en procedures, indien nodig). | VV, V |
| *Gerelateerde kernelementen van de AVG:*   * Rechtmatigheid van de verwerking | | |

|  |  |  |
| --- | --- | --- |
| Periodiek monitoren van privacybeheersingsmaatregelen (MON)  *Beheersingsdoelstelling:*  Systematische en periodieke evaluatie van privacyprocessen en beheersingsmaatregelen waarborgt dat deze naar behoren werken, zodat blijvend wordt voldaan aan de van toepassing zijnde wet- en regelgeving. | | |
| *Fase informatielevenscyclusmanagement:* **Monitoren en handhaven** | | |
| *Beheersingsmaatregelen:* | |  |
| MON01 | Het management van de entiteit evalueert de volgende zaken om de werking van privacybeheersingsmaatregelen te waarborgen:   1. control outputs, controlerapporten en deviaties; 2. trendanalyse; 3. aanwezigheid bij trainingen en evaluaties; 4. klachten en oplossing daarvan; 5. interne beoordelingen; 6. interne en externe auditrapporten; 7. onafhankelijke audit/assurance-rapporten met betrekking tot privacybeheersingsmaatregelen bij dienstverlenende organisaties; 8. andere informatie met betrekking tot de doeltreffendheid van de beheersingsmaatregelen. | VV, V |
| MON02 | De entiteit beslist op basis van de gevoeligheid van de betreffende  persoonsgegevens en het risico op blootstelling of verlies welke  beheersingsmaatregelen worden gemonitord, beoordeeld en/of  gecontroleerd, hoe en met welke frequentie dit gebeurt . | VV, V |
| MON03 | De entiteit heeft een proces ingericht om te waarborgen dat het monitoren resulteert in herstel van tekortkomingen en continue verbetering. | VV, V |
| *Gerelateerde kernelementen van de AVG:*   * Rechtmatigheid van de verwerking | | |