Privacy supplement

BIO Thema-uitwerking

Januari 2022 [versie 1.0 definitief]

BIO Thema-uitwerking Privacy supplement

Titel	BIO Thema-uitwerking Privacy supplement
Datum	Januari 2022
Versie	1.1.0 definitief
Opdrachtgever	Voorzitter werkgroep BIO en directeur CIP
Regime	Becommentarieerde praktijk
Auteurs	CIP Kernteam
Reviewers	Versie 1.0: CIP Kernteam

Versie en status	Datum	Auteur	Distributie	Wijziging
0.1 in bewerking	23/12/2021	CIP Kernteam		Gereviewde opzet
1.0 definitief	4/01/2022	CIP Kernteam		

Considerans

CIP-producten steunen op kennis van professionals uit verschillende organisaties actief in het CIP-netwerk, zowel uit de overheid als de markt.

Opmerkingen en aanvullingen kun je melden op cip-overheid.nl/contact.

Leeswijzer

- Voor de aanduiding van personen wordt de mannelijke vorm aangehouden (hij/hem/zijn) ongeacht het geslacht.
- Van best practices (open standaarden al dan niet toegankelijk met een licentie) zijn de meest actuele versies afgekort vermeld, tenzij de actuele versie niet toereikend is.
- Voor een overzicht van alle gebruikte best practices, afkortingen en begrippen en een generieke toelichting op de opzet van de thema-uitwerkingen, zie de Structuurwijzer BIO Thema-uitwerkingen.

Inhoudsopgave

1 Inleiding

Dit document bevat een aantal eisen voor privacybescherming. Deze eisen zijn van belang om na te leven binnen de (overheids-)organisatie en ook door haar leveranciers zoals shared service centra en marktpartijen.

1.1 Context

De uitwerking van de privacy-maatregelen in dit document is een aanvulling op de uitwerking van de informatiebeveiliging in de diverse BIO thema's, die al beschikbaar gesteld zijn door CIP.

Dit document bevat de privacy-maatregelen die generiek zijn en dus voor alle thema-uitwerkingen gelden maar ook de privacy-maatregelen die alleen voor specifieke thema's gelden.

De beschrijving van de verschillende objecten binnen de privacy-maatregelen heeft dezelfde opbouw en structuur als de objecten binnen de verschillende informatiebeveiliging domeinen van de thema-uitwerkingen.

De objecten uit de privacy-maatregelen zijn gebaseerd op:

- de privacy by design principes uit zoals bedoeld in de "Kamerbrief over privacy by design en open source" van 9 februari 2021;
- de privacy by design principes van Enisa;
- de ISO 27701;
- de AVG.

In de controls en onderliggende maatregelen wordt verwezen naar de AVG maar ook naar andere normenkaders om een samenhangende beschrijving aan te bieden. Vaak wordt ook verwezen naar de CIP Privacy Baseline. Indien geen verwijzing voorhanden is maar de auteurs de maatregel toch van wezenlijk belang achten om een volledig beeld te creëren, is de verwijzing "CIP-netwerk" opgenomen.

1.2 Doel

De uitwerking van de privacy-maatregelen geeft inzicht aan zowel de opdrachtgever als de opdrachtnemer betreffende de eisen waaraan voldaan moet worden om de juiste beveiligingseisen in het privacy domein af te dekken.

De privacy-maatregelen zijn onverkort overgenomen in de ICO-Wizard om ze ook te kunnen meenemen als eisen aan de leverancier bij inkoop en aanbesteding.

1.3 Scope en begrenzing

De uitwerking van de privacy-maatregelen geeft – samen met de eisen die al in de basis van de thema's zijn opgenomen - een compleet beeld van alle objecten per thema die relevant kunnen zijn voor een organisatie.

Via de risico analyse die door de specifieke organisatie of het specifieke organisatieonderdeel is uitgevoerd, moet bepaald worden hoe zwaar op de diverse objecten moet worden ingezet.

2 Privacy-maatregelen geldend voor alle thema's

2.1 ALG P.01 Privacybeleid

Definitie

Passende technische en organisatorische maatregelen moeten worden getroffen, zodat duidelijk is hoe de verwerking wordt gewaarborgd en hoe de persoonsgegevens onder meer worden beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Toelichting

De ontwikkeling van het beleid komt cyclisch tot stand, zodat het beleid kan worden bijgestuurd en gecorrigeerd. Bekende voorbeelden van cyclische processen zijn Plan-Do-Check-Act (PDCA) of Observe-Orient-Do-Act (OODA).

Doelstelling	'Privacybeleid' dient ervoor om op organisatie- en strategisch niveau duidelijkheid te geven over de inrichtingskeuzes van privacy en te waarborgen dat de verwerking van gegevens op een rechtmatige wijze plaatsvindt.		
Risico	Het ontbreken van een privacybeleid leidt ertoe dat de organisatie geen duidelijke richtlijnen heeft, waardoor de kans bestaat dat persoonsgegevens onrechtmatig worden verwerkt (waaronder verzamelen, bewerken, inzien et cetera) en de organisatie niet kan aantonen dat deze zorg draagt voor de privacy(rechten) van betrokkenen, waarvan de persoonsgegevens worden verwerkt, en hiermee voldoet aan de privacywetgeving.		
Control	De organisatie heeft privacybeleid en procedures ontwikkeld en vastgesteld, waarin de **verantwoordelijkheid** is vastgelegd op welke wijze persoonsgegevens worden verwerkt, invulling wordt gegeven aan de wettelijke beginselen en hoe in een **cyclisch proces** wordt **vastgelegd** op welke wijze **transparant** aan de **wet- en regelgeving** wordt voldaan en **afwijkingen** worden opgelost.		AVG: art. 5, 24, 40, UAVG: art. 2, 4, 78 en 157, CIP De Privacy Baseline 2020[1]: B.01
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Verantwoordelijkheid	1.	Het beleid geeft duidelijkheid over hoe de verantwoordelijken hun verantwoordelijkheid voor de naleving van de beginselen en de rechtsgrondslagen invullen, dit kunnen aantonen ("verantwoordingsplicht") en hoe passende technische en organisatorische beveiligingsmaatregelen worden getroffen.	AVG: art. 28, CIP De Privacy Baseline 2020: B.01/01.01, B.01/02.05 en U.04
Cyclisch proces	2.	Het/de privacybeleid, -procedures, -standaarden en -maatregelen zijn tot stand gekomen langs een vastgelegd beschreven cyclisch proces dat voldoet aan een gestandaardiseerd patroon met daarin de elementen: voorbereiden, ontwikkelen, goedkeuren, communiceren, uitvoeren, implementeren en evalueren.	CIP De Privacy Baseline 2020: B.01/01.02, ISO 27002 2017: 5.1.2 en 18.2.2

[1] https://www.cip-overheid.nl/media/1554/20201027_privacybaseline3_3.pdf

Vastgelegd	3.	Het topmanagement van de organisatie heeft het privacybeleid vastgelegd, bekrachtigd en gecommuniceerd binnen de organisatie, met daarin de visie op privacybescherming en richtlijnen voor het (volgens de wet) rechtmatig, behoorlijk en transparant verwerken van persoonsgegevens.	CIP De Privacy Baseline 2020: B.01/01.03
Transparant	4.	Beschreven is hoe gewaarborgd wordt dat de persoonsgegevens op een wijze worden verwerkt die voor het publiek en de betrokkene, waarvan de persoonsgegevens worden verwerkt, transparant is en het deze betrokkene mogelijk maakt zijn rechten uit te oefenen.	CIP De Privacy Baseline 2020: B.01/02.06, U.05 en C.02
Wet- en regelgeving	5.	De organisatie behoort een overzicht op te stellen en bij te houden van relevante aan privacy gerelateerde wet- en regelgeving en de specifieke onderdelen daarvan die relevant zijn voor de te leveren diensten.	NEN 7510 2017: A.18.1.1, CIP De Privacy Baseline 2020: B.01/01.04
Afwijkingen	6.	Bij afwijkingen op de naleving van aan privacy gerelateerde wet- en regelgeving, implementeert en documenteert de organisatie correctieve maatregelen om de afwijking op te lossen.	ENISA strategie 'Aantonen': https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design
Wie	Opdrachtgever en opdrachtnemer		
Wat	Proces		
Verificatie	Overleg bewijsstukken en/of verklaring		

2.2 ALG P.02 Privacy-organisatie

Definitie

Het waarborgen van de privacy ligt niet bij één persoon. Een veelheid van personen binnen een organisatie is betrokken om aan de vereisten van de wet- en regelgeving te kunnen voldoen. De eindverantwoordelijke is degene die het doel en de middelen van de gegevensverwerking heeft vastgesteld.

Toelichting

De rollen zijn duidelijk, doordat de taken, verantwoordelijkheden en bevoegdheden belegd zijn in een TVB-matrix waarbij ook de onderlinge relaties tussen de verschillende verantwoordelijken en verwerkers inzichtelijk zijn gemaakt. De eisen gelden zowel voor binnen een staande organisatie, tussen organisaties als voor projecten en projectprogramma's.

Bij gegevensuitwisseling tussen twee verwerkingsverantwoordelijken wordt een overeenkomst of convenant gesloten, waarin de betrokken partijen afspraken over de gegevensdeling vastleggen, bijvoorbeeld dat de deling van de gegevens rechtmatig is en veilig plaatsvindt. Er moet altijd een geldige grondslag zijn voor het verwerken van de persoonsgegevens en uiteraard geldt dit ook voor de verwerking voor een ander doel. De ontvangende partij is zelf verantwoordelijk voor de technische en organisatorische maatregelen die voor de beveiliging van de gegevens nodig zijn.

Doelstelling	Het doel van een heldere verdeling van taken en bevoegdheden, van middelen en rapportagelijnen is waarborgen dat op de juiste wijze invulling wordt gegeven aan de eisen van het privacybeleid en de AVG.		
Risico	Door het ontbreken van een goede en inzichtelijke taakverdeling en de daarvoor benodigde middelen en rapportagelijnen is niet altijd duidelijk wie wat moet doen, waardoor de eisen van de AVG, de sectorspecifieke wetgeving en het privacybeleid niet effectief worden ingevuld.		
Control	De verdeling van de taken en **verantwoordelijkheden**, de **benodigde middelen** en de **rapportagelijnen**, zijn door de organisatie vastgesteld en vastgelegd, inclusief die bij uitwisseling van persoonsgegevens **tussen organisaties**, zodat ook bij **doorgifte** van persoonsgegevens de privacybelangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, zijn gewaarborgd.		ISO 27701 2019: 6.3.1.1, CIP De Privacy Baseline 2020: B.02
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Verantwoor-delijkheden	1.	Alle relevante rollen en verantwoordelijkheden voor privacy zijn beschreven en toe te kennen aan de betrokken medewerkers. Het is te allen tijde duidelijk wie de verantwoordelijke is.	CIP De Privacy Baseline 2020: B.02/01.01
Benodigde middelen	2.	Gekoppeld aan het privacybeleid voorziet de organisatie voldoende en aantoonbaar in de benodigde middelen voor de uitvoering ervan.	CIP De Privacy Baseline 2020: B.02/02
Rapportagelij-nen	3.	De rapportage- en verantwoordingslijnen tussen de betrokken verantwoordelijken, verwerkers en de Functionaris Gegevensbescherming zijn vastgesteld en vastgelegd.	CIP De Privacy Baseline 2020: B.02/03
Tussen organisaties	4.	In samenwerkingsverbanden, uitbestedingen en dienstverleningen is duidelijk wie verwerkingsverantwoordelijk is of zijn, wie verwerkers zijn en of er sprake is van een gezamenlijke verwerkingsverantwoordelijkheid. Bij een gezamenlijke verwerkingsverantwoordelijkheid is de ontvangende partij zelf verantwoordelijk voor de technische en organisatorische maatregelen die voor de beveiliging van de gegevens nodig zijn.	Schema 3 van de Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming: https://www.rijksoverheid.nl/documenten/rapporten/2018/01/22/handleiding-algemene-verordening-gegevensbescherming
Doorgifte	5.	Beschreven is hoe gewaarborgd wordt dat persoonsgegevens slechts worden doorgegeven wanneer formeel afdoende garanties zijn vastgelegd zodat aangetoond kan worden dat ook bij de doorgifte aan de AVG wordt voldaan en wat in verwerkers-overeenkomsten en samenwerkingsovereenkomsten moet worden vastgelegd.	CIP De Privacy Baseline 2020: B.01/02.06 en U.07
Wie	Opdrachtgever en opdrachtnemer		
Wat	Proces		

Verificatie	Overleg bewijsstukken en/of verklaring

2.3 ALG P.03 Privacy-bewustzijn

Definitie

Privacy is niet van één persoon. Je kunt privacy nog zo goed inregelen, als het besef ontbreekt bij de mensen die het moeten ondersteunen, kan dat andere principes gemakkelijk teniet doen. Voor het welslagen van het beschermen van privacy van betrokkenen, waarvan de persoonsgegevens worden verwerkt, is het nemen en hanteren van privacy-maatregelen door eenieder die persoonsgegevens verwerkt of een verwerking voorbereid van belang. Randvoorwaarden om te slagen zijn duidelijkheid, kennis en bewustzijn. Dit kan ontstaan via privacybeleid en awareness- en kennistrainingen. Zo wordt privacy een gedeelde verantwoordelijkheid.

Toelichting

Bij iedere maatregel moet verder gekeken worden dan alleen het uitvoeren ervan, vastgesteld moet worden of het beoogde resultaat voor de betrokkene, waarvan de persoonsgegevens worden verwerkt, zich daadwerkelijk voordoet. Het correctierecht, het laten staken van de verwerking van zijn of haar gegevens en het uitwissen van de gevolgen voor de persoonlijke levenssfeer van deze betrokkene zijn voorbeelden, waarbij de persoonlijke levenssfeer kan worden beschermd. Een collectief bewustzijn van het belang van privacy en hoe dit de persoonlijke levenssfeer van deze betrokkenen kan beïnvloeden, de betekenis van maatregelen, wetenschap van de verantwoordelijkheden van de organisatie en de benodigde kennis, zijn alle nodig om de maatregelen effectief te maken.

Doelstelling	Eenieder die persoonsgegevens verwerkt of een verwerking voorbereid is zich bewust van de belangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, en beschouwt dit als hoogste prioriteit om deze overtuiging toe te passen en heeft daarvoor de benodigde kennis.		
Risico	Door een tekort aan bewustzijn, kennis of informatie binnen de organisatie, binnen projecten en bij medewerkers en relevante derden vindt inbreuk op de privacy van betrokkenen, waarvan de persoonsgegevens worden verwerkt, plaats.		
Control	De organisatie waarborgt dat eenieder die persoonsgegevens verwerkt of een verwerking voorbereidt zich bewust is van de belangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, en beschouwt dit conform de **verwachtingen** als hoogste prioriteit om deze overtuiging **toe te passen**; deze betrokkenen hebben daarvoor de benodigde **kennis** en zijn op de hoogte van grote **veranderingen** in de verwachtingen.		AVG: art. 32, ISO 27701 2019: 6.12.1.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Verwachtingen	1.	De verwachtingen omtrent het beschermen van privacy door de organisatie zijn voor eenieder die persoonsgegevens verwerkt of een verwerking voorbereid, periodiek geïnventariseerd en vastgelegd.	CIP-netwerk
Toe te passen	2.	Eenieder die persoonsgegevens verwerkt of een verwerking voorbereid stelt daartoe passende maatregelen in.	CIP-netwerk

Kennis	3.	Eenieder die persoonsgegevens verwerkt of een verwerking voorbereid heeft het daartoe vereiste kennisniveau en er is een collectief bewustzijn.	CIP-netwerk
Veranderingen	4.	De organisatie heeft een proces vastgesteld en geïmplementeerd voor het periodiek en bij grote veranderingen op de hoogte brengen van de verwachtingen op het gebied van privacy aan eenieder die persoonsgegevens verwerkt of een verwerking voorbereid.	CIP-netwerk
Wie	Opdrachtgever en opdrachtnemer		
Wat	Proces		
Verificatie	Overleg bewijsstukken en/of verklaring		

2.4 ALG P.04 Formele vastlegging handelen verwerker

Definitie

Als een persoon of organisatie namens een verwerkingsverantwoordelijke persoonsgegevens verwerkt, dan moet hij hierover met deze verwerkingsverantwoordelijke een overeenkomst afsluiten. Het gaat daarbij om die situaties waarin de verwerker opdracht krijgt van de organisatie die verantwoordelijk is voor de verwerking van de persoonsgegevens; deze verantwoordelijke opdrachtgever bepaalt wat moet gebeuren met de gegevens en hoe.

Toelichting

-

Doelstelling	Het vaststellen en vastleggen van de verantwoordelijkheden van eenieder die persoonsgegevens verwerkt of een verwerking voorbereid, zodat zij de privacy van betrokkenen, waarvan de persoonsgegevens worden verwerkt, waarborgen en handelen in het belang van de organisatie en deze betrokkenen.		
Risico	De personen die persoonsgegevens verwerken zijn niet gebonden aan de maatregelen, waardoor de privacy en de belangen van betrokkenen, waarvan de persoonsgegevens worden verwerkt, niet zijn gewaarborgd.		
Control	De organisatie heeft van eenieder, die persoonsgegevens verwerkt of een verwerking voorbereidt, een actuele **VOG**, een **actuele verklaring** terzake het naleven en de kennisname van de regels omtrent privacy en het bewijs van op de hoogte zijn van de **disciplinaire procedure**; hiervan bestaat een **overzicht**.		NEN 7510 2017: A.7.1.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
VOG	1.	Het aanvragen van een VOG (Verklaring Omtrent Gedrag) is onderdeel van de sollicitatieprocedure en van een procedure, waarin één keer per jaar, een originele VOG moet worden overlegd. Deze documenten moeten worden bewaard op basis van vastgestelde criteria.	NEN 7510 2017: A.7.1.1

Actuele	2.	Bij grote wijzigingen in regels omtrent privacy worden nieuwe verklaringen getekend door de medewerkers.	CIP-netwerk
Verklaring	3.	Medewerkers tekenen een verklaring voor het naleven en kennisname van de regels omtrent privacy die de organisatie hanteert.	NEN 7510 2017: A.7.1.1
Disciplinaire procedure	4.	Een disciplinaire procedure die wordt ingezet bij het overtreden van regels omtrent privacy is beschreven, geïmplementeerd en gecommuniceerd met de medewerkers.	ISO 27002 2017 7.2.3
Overzicht	5.	De organisatie heeft een overzicht beschikbaar waarin is beschreven welke werknemers een VOG (zie 1.) hebben overlegd, de verklaring (zie 2.) getekend en op de hoogte zijn van de disciplinaire procedure (zie 3.).	AVG: art. 30
Wie	Opdrachtnemer		
Wat	Proces		
Verificatie	Overleg bewijsstukken en/of verklaring		

2.5 ALG P.05 Privacy in de levenscyclus

Definitie

Het borgen van het privacybelang van betrokkenen, waarvan de persoonsgegevens worden verwerkt, en het voldoen aan de wet- en regelgeving is een continu proces dat de privacyrisico's signaleert dit start bij de eerste plannen voor het ontwikkelen van een gegevensverwerking en pas stopt nadat de persoonsgegevens en de gegevensverwerking zijn verwijderd. Hierbij moet continu beoordeelt worden of het privacybelang van deze betrokkenen is geborgd en een passende behandeling daarvan wordt bewaakt, zodat bij het ontwerp, de ontwikkeling, de inrichting en de inzet van de gegevensverwerking voor de organisatie de privacyrisico's in lijn zijn gebracht met het privacybeleid.

Toelichting

De levenscyclus van verwerkingen en het komen tot deze verwerkingen bevat de fasen van het plannen van een verwerking, het ontwerp, de ontwikkeling, het testen, de acceptatie, de productie (de verwerking zelf) en exit van (potentiële) verwerkingen. De Privacy by Design (PbD) principes die daarbij gehanteerd worden zijn gebaseerd op:

a) Voorkomen is beter dan genezen;
b) Privacy is de standaard;
c) Integreren van gegevensbescherming en beveiliging in het ontwerp;
d) Volledige functionaliteit;
e) End-to-end beveiliging;
f) Zichtbaarheid en transparantie;
g) Respect voor privacy van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, staat centraal.

De Privacy by design en privacy by default verplichting geldt voor:

a) De hoeveelheid verzamelde persoonsgegevens;
b) De mate waarin zij worden verwerkt;

c) De termijn waarvoor zij worden opgeslagen;
d) De toegankelijkheid daarvan.

Doelstelling	Het tijdig beoordelen van de privacyrisico's (de kans en hun potentiële omvang/impact), zodat bepaald kan worden hoe deze, door het treffen van maatregelen, teruggebracht kunnen worden tot binnen grenzen die de verwerkingsverantwoordelijke acceptabel acht.		
Risico	Privacyrisico's worden niet of niet tijdig gesignaleerd zodat een grote(re) kans op inbreuken op de beveiliging en schade voor natuurlijke personen ontstaat van wie de persoonsgegevens onrechtmatig worden verwerkt.		
Control	**Vooraf** aan het ontwerp van een gegevensverwerking en bij een **verandering** wordt een inschatting gemaakt van de privacyrisico's en wordt bepaald welke **passende maatregelen** nodig zijn; hiervoor zijn de **verantwoordelijkheden** duidelijk en is een **proces** ingeregeld voor het kunnen aantonen van het passend zijn van deze maatregelen.		ISO 27002 2017: 7.2.3
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Vooraf	1.	Wanneer een hoog risico voor de rechten en vrijheden van natuurlijke personen bestaat, in het bijzonder wanneer gelet op de aard, de omvang, de context en de doeleinden nieuwe technologieën worden gebruik, wordt voorafgaand aan de verwerking een gegevensbeschermingseffectbeoordeling (DPIA) uitgevoerd.	AVG: art. 35, CIP De Privacy Baseline 2020: B.03/01.01
Verandering	2.	Ten minste wanneer sprake is van een verandering van het risico dat de verwerkingen inhoudt, verricht de verwerkingsverantwoordelijke een toetsing om te beoordelen of de verwerking overeenkomstig de gegevensbeschermingseffectbeoordeling (DPIA) wordt uitgevoerd.	AVG: art. 35, CIP De Privacy Baseline 2020: B.03/01.03
Passende maatregelen	3.	Passende maatregelen zijn genomen door bij het ontwerp de principes van gegevensbescherming te hanteren (privacy by design) en door het hanteren van standaardinstellingen (privacy by default).	AVG: art. 25, CIP De Privacy Baseline 2020: B.03/02.02
Verantwoor-delijkheden	4.	Beschreven is hoe en door wie gewaarborgd wordt dat verantwoordelijken aantoonbaar maatregelen hebben genomen door het toepassen van Privacy by Design, het uitvoeren van DPIA's en het gebruik van standaard instellingen.	CIP De Privacy Baseline 2020: B.01/01.02 en B.03
Proces	5.	Er is een proces ingeregeld voor het toepassen van Privacy by Design principes en Privacy by Default binnen de volledige levenscyclus van oplossingen en het komen tot deze oplossingen.	PbD principe integreren van gegevensbescherming en beveiliging in het ontwerp
Wie	Opdrachtgever en opdrachtnemer		
Wat	Proces		
Verificatie	Overleg bewijsstukken en/of verklaring		

2.6 ALG P.06 Register van verwerkingsactiviteiten

Definitie

De AVG verplicht het opstellen en up-to-date houden van een 'Register van verwerkingsactiviteiten', tenzij de omvang van de organisatie en de gevoeligheid beperkts is (AVG: art. 30). Het register maakt toezicht op de verwerkingsactiviteiten mogelijk. Het Register van verwerkingsactiviteiten wordt doorgaans aangeduid als verwerkingsregister.

Toelichting

Om de naleving van de AVG aan te kunnen tonen, dient de verwerkingsverantwoordelijke of de verwerker, een register bij te houden van verwerkingsactiviteiten die onder zijn verantwoordelijkheid hebben plaatsgevonden. Het bijhouden van het register kan worden uitgevoerd door een gecentraliseerd onderdeel. Dit verbetert de mogelijkheden een actueel en samenhangend beeld te geven.

Wat in het register beschreven moet zijn, staat in AVG: art. 30 lid 1. Dit is inclusief een algemene beschrijving van de genomen technische en organisatorische beveiligingsmaatregelen.

Doelstelling	Het doel van een Register van verwerkingsactiviteiten is inzicht te verstrekken in de verwerkingen en de gegevensstromen binnen de organisatie en bij de partijen die namens de organisatie zorgen voor de verwerking van persoonsgegevens.		
Risico	Het niet hebben van een overzicht van verwerkingen leidt tot een incompleet beeld van de verwerkte categorieën persoonsgegevens en getroffen maatregelen voor de relevante verwerkingen, processen en technische systemen, waardoor niet kan worden aangetoond dat de organisatie aan de privacyregels voldoet.		
Control	De **verwerkingsverantwoordelijke(n) en de verwerker(s)** hebben hun gegevens over de gegevensverwerkingen in een register **vastgelegd**, daarbij biedt het **register** een **actueel** en **samenhangend** beeld van de gegevensverwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens en dat voldoet aan de **vereisten** van de AVG**.**		AVG: art. 30
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Verwerkings-verantwoor-delijke(n) en de verwerker(s)	1.	Het is de verwerkingsverantwoordelijke(n) en de verwerker(s) duidelijk of de AVG een Register van verwerkingsactiviteiten voorschrijft.	AVG: art 1., https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verantwoordingsplicht#ben-ik-verplicht-om-een-verwerkingsregister-op-te-stellen-7191
Vastgelegd	2.	Beschreven is hoe gewaarborgd wordt dat de verwerking van de persoonsgegevens behoorlijk is en hoe dit via het bijhouden van een register en een dossier kan worden aangetoond.	CIP De Privacy Baseline 2020: B.01/02.09 en C.01

Register	3.	De verwerkingsverantwoordelijke(n) en de verwerker(s), waarvoor een Register van verwerkingsactiviteiten is voorgeschreven, houden een register bij voor hun verwerkingen van persoonsgegevens.	AVG: art. 30
Actueel	4.	De verwerker verschaft de verwerkingsverantwoordelijke het door de AVG vereiste inzicht en doet dit in een voor de verwerkingsverantwoordelijke verwerkbare vorm, zodat het register actueel gehouden kan worden.	CIP-netwerk
Samen-hangend	5.	De Register van verwerkingsactiviteiten van de verwerkingsverantwoordelijke en van de verwerker geven één samenhangend beeld.	AVG: art. 30.
Vereisten	6.	Het Register van verwerkingsactiviteiten voldoet aan de vereisten van de AVG: art. 30 lid 1.	AVG: art. 30 lid 1, Autoriteit Persoonsgegevens: Verantwoordingsplicht: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verantwoordingsplicht#wat-moet-er-in-het-verwerkingsregister-staan-7193
Wie	Opdrachtgever en opdrachtnemer		
Wat	Proces		
Verificatie	Overleg bewijsstukken en/of verklaring		

2.7 ALG P.07 Datalekken

Definitie

Het bieden van inzicht in een datalek en de mogelijke gevolgen ervan kan mogelijk (negatieve) consequenties voor de betrokkenen, waarvan de persoonsgegevens worden verwerkt, beperken. Een datalek is een "inbreuk vanwege persoonsgegevens": een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Toelichting

Het gaat in de AVG om twee verschillende meldplichten: 1. een meldplicht aan de AP en 2. een meldplicht aan de betrokkene, waarvan de persoonsgegevens worden verwerkt, en dus op wiens persoonsgegevens een inbreuk is gemaakt. De AVG hanteert een aantal uitzonderingsgronden, waarbij het datalek niet gemeld hoeft te worden.

De documentatie bevat de noodzakelijke gegevens van alle datalekken, ook die welke niet gemeld zijn. Desgevraagd moet meer documentatie voorhanden zijn die direct in verband staat met de melding van een inbreuk zelf. Nagegaan moet kunnen worden of alle passende technische en organisatorische maatregelen zijn genomen om vast te stellen of een inbreuk, vanwege persoonsgegevens, heeft plaatsgevonden en om de AP en deze betrokkene daarvan onverwijld in kennis te stellen.

Doelstelling	Het achterhalen van de oorzaak van een datalek, voor het nemen van maatregelen om herhaling te voorkomen en belanghebbenden te informeren.		
Risico	Negatieve consequenties die persoonlijke levenssfeer van de betrokkene, waarvan de persoonsgegevens worden verwerkt, treffen.		
Control	De organisatie heeft de **kennis** georganiseerd om de **oorzaak** van een datalek te kunnen vaststellen en te onderzoeken, heeft daarvoor de benodigde **loggegevens** om **herhaling** te voorkomen en heeft de **stakeholders vastgesteld** om ze te kunnen **informeren**.		AVG: art.33
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Kennis	1.	De organisatie beschikt zelf over medewerkers met voldoende kennis om de oorzaak van een datalek te kunnen achterhalen of heeft toegang tot een externe partij die de oorzaak kan achterhalen.	CIP-netwerk
Oorzaak	2.	De organisatie heeft een proces beschreven en geïmplementeerd voor het achterhalen van de oorzaak van een datalek, hierbij is de inbreuk gedocumenteerd met alle noodzakelijke gegevens van alle datalekken.	CIP De Privacy Baseline 2020: C.03/03
Loggegevens	3.	De organisatie heeft inzicht in welke loginformatie van de applicatie nodig is, om (een deel van) de oorzaak van een datalek, gerelateerd aan de applicatie, te kunnen achterhalen.	CIP-netwerk
Herhaling	4.	De organisatie heeft een proces beschreven en geïmplementeerd voor het evalueren van datalek-incidenten en het nemen van maatregelen ter voorkoming van herhaling van datalek-incidenten en de vastlegging daarvan.	CIP-netwerk
Stakeholders vastgesteld	5.	De organisatie heeft vastgesteld wie de relevante stakeholders (kunnen) zijn, waaraan de melding van (potentiële) datalekken moet plaatsvinden, er gelden wettelijke uitzonderingsgronden.	CIP De Privacy Baseline 2020: C.03/04
Informeren	6.	Beschreven is hoe gewaarborgd wordt dat bij een datalek de stakeholders en zo nodig de betrokkenen, waarvan de persoonsgegevens wordt verwerkt, en de AP worden geïnformeerd als deze inbreuk waarschijnlijk een risico inhoudt voor de rechten en/of vrijheden van natuurlijke personen.	AVG: art. 33, CIP De Privacy Baseline 2020: B.01/02.10 en C.03/01
Wie	Opdrachtnemer		
Wat	Proces		
Verificatie	Overleg bewijsstukken en/of verklaring		

3 Privacy-maatregelen Toegangsbeveiliging

3.1 TBV P.01 Stelsel van toegangsbeheer

Definitie

Het uitgangspunt van toegang op basis van doelbinding is, dat persoonsgegevens toegankelijk zijn voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigde doel. 'Welbepaald en uitdrukkelijk omschreven' houdt in dat men geen gegevens mag verwerken zonder een precieze doelomschrijving. Het doel moet zijn bepaald alvorens men tot verzamelen overgaat.

'Welbepaald' houdt in dat deze doelomschrijving duidelijk moet zijn, niet zo vaag of ruim dat zij tijdens het verzamelproces geen kader kan bieden waaraan getoetst kan worden of de gegevens nodig zijn voor dat doel of niet. Dit geldt daarmee ook voor de toegang tot de gegevens.

Het doel van de toegang moet uitdrukkelijk zijn omschreven en houdt in dat de verantwoordelijke het doel waarvoor hij verwerkt moet hebben omschreven.

Doelbinding is een belangrijk uitgangspunt bij het verstrekken van toegang als privacy-maatregel.

Toegang tot een verwerking moet daartoe een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel hebben. Het toekennen en bewaken van toegang tot persoonsgegevens kan op verschillende manieren gebeuren. De volgende manieren zijn daarin complementair:

- **Toegang op basis van (functie)rollen:**
  Vanuit informatiebeveiliging worden toegangsrechten op basis van rollen toegekend. Het hebben van een rol kan te ruim (‘grofmazig’) zijn om doelbinding af te dwingen.
- **Toegang op basis van taken:**
  Doelbinding is altijd gerelateerd aan de verwerking die uitgevoerd moet worden. De verwerking en de toegang tot de daarvoor benodigde persoonsgegevens is dan gebaseerd op de toegekende taak. De taak gebaseerde toegang is daarmee fijnmaziger dan de rol gebaseerde toegang. Dit fijnmazige karakter is enerzijds de fijnmazigheid in de verzameling van verwerkingen en in gegevens en anderzijds fijnmazigheid in de tijd. De toegang kan namelijk beperkt worden tot alleen het moment dat een taak uitgevoerd moet worden.
- **Logging en monitoring:**
  Het toekennen van toegangsrechten op basis van rollen en taken moet worden gelogd en gemonitord. Daarnaast kan de gebruikte toegang tot een verwerking en een persoonsgegeven worden gelogd en gemonitord. Logging en monitoring biedt zo de mogelijkheid de legitimiteit van de toegang te bewaken, vast te leggen en te toetsen aan de doelbinding.

Toelichting

Toegang wordt gegeven en beperkt tot alleen die toegang waar op dat moment voor het uitvoeren van een taak binnen een bepaalde rol recht op is. Het is daarmee een proces waarbij de rechten gebaseerd worden op basis van rollen en op de op dat moment uit te voeren taak. Aanvullend kan de gebruikte toegang tot persoonsgegevens worden gelogd, gemonitord en getoetst op rechtmatigheid. Toegangsbeheer is daarmee een stelsel van maatregelen, die in samenhang moet worden ingezet.

Doelstelling	Het beheren van de toegang tot persoonsgegevens op basis van maatregelen, zodat enerzijds de toegang beperkt is tot die taken die gerechtvaardigd zijn en anderzijds ongerechtvaardigde toegang wordt gesignaleerd.

Risico	Het gebruik van een onrechtmatige toegang is een datalek, wat kan leiden tot een inbreuk op de privacy van betrokkenen, waarvan de persoonsgegevens worden verwerkt.		
Control	Het doel van de verwerking van persoonsgegevens en van de toegang zijn **welbepaald, gerechtvaardigd** en uitdrukkelijk **omschreven**, waarbij de toegang naar keuze **rol** gebaseerd en waar nodig **taak** gebaseerd wordt verstrekt. Aanvullend vindt **logging en monitoring**plaats.		AVG: art. 5
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Welbepaald, gerecht-vaardigd	1.	Van alle gegevens, waartoe toegang wordt verstrekt, zijn de rechtmatige gronden en de doeleinden van de verzameling en verwerking welbepaald en uitdrukkelijk omschreven en gerechtvaardigd.	AVG: art. 5 lid 1b
Omschreven	2.	Het doel van de toegang is welbepaald en uitdrukkelijk omschreven, dus niet te vaag of te ruim, maar nauwkeurig, specifiek, meetbaar, acceptabel, realistisch en tijdsgebonden.	AVG: art. 5 lid 1 en overweging 50
Rol	3.	Bepaald is welke toegangsrechten op basis van rollen kunnen worden afgedwongen.	AVG: art. 5
Taak	4.	Bepaald is welke toegangsrechten aanvullend beperkt moeten worden op basis van tijdelijkheid en een taak binnen de rol.	AVG: art. 5
Logging en monitoring	5.	Bepaald is welke toegang tot verwerkingen en persoonsgegevens moet worden gelogd, gemonitord en getoetst, zodat bepaald kan worden of de toegang steeds rechtmatig is geweest.	CIP-netwerk
Wie	Opdrachtnemer		
Wat	Product		
Verificatie	Overleg bewijsstukken en/of verklaring		

3.2 TBV P.02 Doelbinding op rolniveau

Definitie

Een verwerker krijgt toegang tot verwerkingen op basis van toegangsrechten. Daarvoor zijn fysieke toegangssystemen, (centraal) authenticatiesystemen en (centraal) autorisatiesystemen ingericht. De rol gebaseerde toegang wordt bijgehouden in het autorisatiesysteem. Wijzigingen treden op bij verandering in de functie, taken of bij contractuele veranderingen, zoals uitdiensttreding.

Toelichting

Functiescheiding in de informatiebeveiliging is met name gericht op het voorkomen van bedrijfsschade. De functiescheiding die nodig is bij privacybescherming gaat verder en is ook gericht op het voorkomen van de kans op profilering.

Doelstelling	Het beperken van de toegang tot die rollen en die verwerkers die taken uitvoeren die gerechtvaardigd zijn.		
Risico	Het gebruik van een onrechtmatige toegang, omdat de toegang niet bij de rol of de verwerker past is een datalek, die kan leiden tot profilering en inbreuk op de privacy van betrokkenen, waarvan de persoonsgegevens worden verwerkt.		
Control	De organisatie behoort verwerkers **gescheiden** en **beperkt** toegang te **verlenen** tot persoonsgegevens, op basis van uit te voeren activiteiten die binnen een specifieke rol worden uitgevoerd en **in te trekken**, indien de activiteiten, noodzaak of vastgestelde doelbinding niet meer geldt voor deze persoon of rol; de verstrekte toegang is **toetsbaar**.		NEN 7510 2017: A.9.2.6
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Gescheiden	1.	De rollen zijn zodanig vastgesteld dat zij functiescheiding mogelijk maken, zodat door een verwerker geen persoonsgegevens kunnen worden gekoppeld en ongewenste profilering mogelijk is.	ENISA strategie 'Scheiden': https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design, BIO Thema-uitwerking Toegangsbeveiliging 2020: U.07[2]:
Beperkt	2.	Verwerkers worden op basis van de juiste (functie)rollen geautoriseerd voor het gebruik van applicaties.	BIO Thema-uitwerking Toegangsbeveiliging 2020: U.01
Verlenen	3.	De organisatie verleent verwerkers toegang tot persoonsgegevens, op basis van rollen, waarvoor een doelbinding geldt.	CIP-netwerk
In te trekken	4.	De organisatie trekt op persoonsgegevensniveau de toegang tot de gegevens in, zodra de doelbinding waarop de toegang was gebaseerd, voor deze rol of verwerker niet meer bestaat.	CIP-netwerk
Toetsbaar	5.	Het doel en het verstrekken van de toegang is zodanig vastgelegd (welbepaald) dat het een kader biedt waaraan getoetst kan worden of de toegang noodzakelijk is.	AVG: art. 6 lid 4
Wie	Opdrachtgever en opdrachtnemer		
Wat	Product		
Verificatie	Overleg bewijsstukken en/of verklaring		

[2] https://www.cip-overheid.nl/media/1553/202010-bio-thema-uitwerking-toegangsbeveiliging-v20-def.pdf

3.3 TBV P.03 Toegang op taakniveau

Definitie

Dit object beschrijft de eisen die aan de toegang tot verwerkingen worden gesteld, waarbij de toegang gespecificeerd wordt tot op taakniveau. Een verwerking mag immers alleen plaatsvinden voor een specifiek doel, ofwel een specifieke taak. Het is daarmee een aanvulling op de toegang op basis van rollen.

De toegang op basis van rollen wordt doorgaans in een toegangsbeveiligingssysteem bijgehouden. Doordat doelbinding een taakgebonden karakter heeft en het taakgebonden karakter tijdsgebonden is, kan dit niet ondersteund worden vanuit een toegangsbeveiligingssysteem, maar zal de toegang op taakniveau binnen de applicatie geregeld moeten worden.

Taken worden vaak toegekend op basis van het behandelen van een dossier. In dat geval spreekt men ook wel van dossiergebonden toegang.

Toelichting

De toegang op basis van rollen is niet fijnmazig en slechts beperkt tijdsgebonden. De op basis van rollen uitgegeven toegangsrechten geven daardoor ook toegang tot persoonsgegevens die voor het op dat moment geldende doel niet gerechtvaardigd zijn. Door toegang taakgebonden en daarmee ook meer tijdsgebonden te maken, meer dan het geval is als dit op basis van rollen gebeurt, wordt de toegang steeds specifiek voor één verwerkingsdoel verstrekt.

Het tijdsgebonden karakter van toegang op taakniveau vraagt om het toekennen van toegangsrechten op taakniveau binnen de applicatie. Welke toegangsrechten binnen de applicatie worden beheerd en welke op die binnen een (centraal) autorisatiesystemen wordt bepaald tijdens de ontwikkeling van de applicatie.

Doelstelling	Het verstrekken van toegang tot persoonsgegevens, waarvan de toegang is gebaseerd op rechtvaardige gronden, die tijdsgebonden zijn.	
Risico	De toegang op basis van rollen is niet fijnmazig en slechts beperkt tijdsgebonden, waardoor de uitgegeven toegangsrechten op basis van rollen ook toegang geven tot persoonsgegevens die voor het op dat moment geldende doel niet gerechtvaardigd zijn, waardoor voor een verwerking geen rechtmatige grond bestaat.	
Control	Het verlenen van toegang tot persoonsgegevens wordt **beperkt** op basis van duidelijke en afgebakende **taken** en het doel en de verstrekte toegang is **toetsbaar**.	CIP-netwerk
Conformiteitsindicator		**Afgeleid/afkomstig van**

Beperkt	1.	De taken zijn zodanig vastgesteld dat zij het fijnmazig en tijdsgebonden toestaan van de toegang tot persoonsgegevens mogelijk maken, zodat een verwerker geen persoonsgegevens kan inzien die niet nodig zijn voor het uitvoeren van zijn (op dat moment toegewezen) taak.	ENISA strategie (January 12, 2015) 'minimalisatie': https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design, BIO Thema-uitwerking Toegangsbeveiliging 2020: U.07
Taken	2.	De rechten die zijn beperkt op basis van taken worden beheerd binnen de applicatie.	CIP-netwerk
Toetsbaar	3.	Het doel en het verstrekken van de toegang is zodanig vastgelegd (welbepaald) dat het een kader biedt waaraan getoetst kan worden of de toegang noodzakelijk is.	AVG: art. 6 lid 4
Wie	Opdrachtgever en opdrachtnemer		
Wat	Product		
Verificatie	Overleg bewijsstukken en/of verklaring		

3.4 TBV P.04 Logging en monitoring uitgeven toegangsrechten

Definitie

Logging is bij het beheren van de toegang tot persoonsgegevens een methode voor het bijhouden en opslaan van informatie over bijvoorbeeld wie toegang heeft gehad en wanneer. Gedurende het monitoren wordt beoordeeld of de toegang rechtmatig is en dus aan de doelbindingseisen voldoet.

Toelichting

In de te ontwikkelen verwerkingssystemen moeten faciliteiten voor logging en monitoring zijn ingebouwd die ertoe bijdragen dat rechtmatige en onrechtmatige pogingen om persoonsgegevens in te zien of te wijzigen gedetecteerd en vastgelegd worden.

Doelstelling	Onrechtmatige pogingen om persoonsgegevens in te zien of te wijzigen worden tijdig gedetecteerd en vastgelegd, zodat via de logregistratie de oorzaak van een datalek kan worden achterhaald of daar een bijdrage aan kan leveren en onrechtmatige pogingen worden ontmoedigd of zelfs voorkomen.
Risico	Het niet kunnen signaleren van onrechtmatige pogingen om toegang te krijgen vergroot de kans op datalekken, dan wel maakt het moeilijk om de oorzaak/veroorzaker van een datalek te achterhalen.

Control	De verwerking behoort op verwerkers/persoonsniveau te **loggen**, zodat direct of **periodiek** kan worden **beoordeeld** welke persoonsgegevens de medewerker heeft opgevraagd, ingezien en aangepast.		AVG: art. 5 lid 2 en art. 33 lid 5
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Loggen	1.	De verwerkingen, waarin persoonsgegevens worden gebruikt, houden een logregistratie bij, waarin op persoonsniveau duidelijk is op welk tijdstip en wie toegang had tot deze persoonsgegevens.	CIP-netwerk
Periodiek	2.	De logbestanden moeten op vastgestelde tijdstippen worden beoordeeld.	CIP De Privacy Baseline 2020: U.01
Beoordeeld	3.	De logbestanden worden gedurende een overeengekomen periode bewaard voor toekomstig onderzoek en toegangscontrole.	CIP-netwerk
Wie	Opdrachtnemer		
Wat	Product		
Verificatie	Overleg bewijsstukken en/of verklaring en testen		

3.5 TBV P.05 Toegang tot fysieke omgevingen

Definitie

Fysieke omgevingen bieden een fysieke afscherming van persoonsgegevens.

Fysieke beveiliging kan worden bereikt door het opwerpen van allerlei fysieke barrières rond het bedrijfsterrein en rond de IT-voorzieningen. Elke barrière creëert zo een beveiligde zone waarmee de totale beveiliging wordt versterkt. Een beveiligde zone is een gebied binnen een barrière, zoals muren of hekken, die alleen met een toegangspas of via een bemande receptiebalie geopend kan worden.

Toelichting

De fysiek afscherming van persoonsgegevens wordt verkregen door het beperken van de fysieke toegang tot die medewerkers die daartoe een noodzakelijk belang hebben. De locatie en sterkte van de barrières moeten passend zijn voor de omvang en categorie van persoonsgegevens en daarmee passend zijn voor de stand der techniek.

Doelstelling	Het beperken van de toegang tot de fysieke omgevingen, waar persoonsgegevens worden verwerkt, tot enkel die medewerkers die daartoe een noodzakelijk belang hebben.
Risico	Het ontstaan van een (mogelijke) datalek, doordat onrechtmatig fysieke toegang tot persoonsgegevens wordt verkregen.

Control	De organisatie behoort fysieke beveiliging van omgevingen waar persoonsgegevens worden verwerkt, op **passende wijze** ingericht te hebben, zodat enkel medewerkers met **noodzakelijk belang** toegang hebben tot en zich bevinden in deze omgevingen; de toegang wordt **geregistreerd**.		ISO 27002 2017: 11.1, ABDO 2019 v1.1: 3.1.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Passende wijze	1.	De fysieke beveiliging van omgevingen waar persoonsgegevens worden verwerkt, is op een passende wijze ingericht zodat de toegang wordt beperkt tot enkel die medewerkers die daartoe een noodzakelijk belang hebben.	CIP-netwerk
Noodzakelijk belang	2.	De toegang is beperkt tot enkel die medewerkers die een noodzakelijk belang hebben tot toegang en zich bevinden in omgevingen met persoonsgegevens.	CIP-netwerk
Geregistreerd	3.	Aankomst- en vertrektijden van bezoekers worden geregistreerd.	BIO Thema-uitwerking Toegangsbeveiliging 2020: U.11
Wie	Opdrachtnemer		
Wat	Product		
Verificatie	Overleg bewijsstukken en/of verklaring		

3.6 TBV P.06 Toegang buiten beveiligde omgevingen

Definitie

Persoonsgegevens worden afgeschermd door het bieden van een fysiek beveiligde omgeving.

Toelichting

Buiten de fysieke omgevingen, bijvoorbeeld tijdens transport, kunnen aanvullende maatregelen nodig zijn om een mogelijke datalek te voorkomen.

Doelstelling	Het voorkomen van een (mogelijk) datalek wanneer de persoonsgegevens zich buiten fysiek beveiligde omgevingen bevinden.	
Risico	Het ontstaan van een datalek, doordat geen afdoende maatregelen zijn getroffen, wanneer buiten de beveiligde omgeving fysieke toegang tot de gegevens bestaat of kan ontstaan.	
Control	Er is een **procedure** ingericht voor het transporteren van persoonsgegevens buiten een beschermde omgeving, waarbij door **versleuteling** de kans op een datalek is verkleind en door **minimalisatie** de omvang van een datalek wordt beperkt.	AVG: art. 32
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Procedure	1.	De organisatie heeft een procedure ingericht voor het transporteren van persoonsgegevens buiten de beschermde omgeving, waarin maatregelen zijn ingericht ter bescherming van de privacy van betrokkenen, waarvan de persoonsgegevens worden verwerkt.	AVG: art. 32
Versleuteling	2.	Daar waar het risico bestaat dat persoonsgegevens ingezien kunnen worden door onbevoegden worden gegevens verborgen, door het toepassen van versleuteling.	ENISA Privacy and Data Protection by Design (January 12, 2015) 'Verbergen: www.enisa.europa.eu/publications/privacy-and-data-protection-by-design
Minimalisatie	3.	De persoonsgegevens die buiten de beveiligde omgevingen wordt gebracht worden beperkt tot alleen die gegevens die noodzakelijk zijn voor het vooraf vastgelegde doel van het transporteren.	ENISA Privacy and Data Protection by Design (January 12, 2015) 'Minimaliseren': https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design
Wie	Opdrachtgever en opdrachtnemer		
Wat	Proces		
Verificatie	Overleg bewijsstukken en/of verklaring		

3.7 TBV P.07 Toegang in het buitenland

Definitie

De bescherming van persoonsgegevens is niet in alle landen hetzelfde geregeld. Bij reizen in het buitenland is er, wanneer een buitenlandse overheid daarin geïnteresseerd is en vooral als zij door de uitoefening van buitenlandse wetgeving die privacyrisico's met zich meebrengt, een vergrote kans dat toegang tot vertrouwelijke informatie, in deze persoonsgegevens, wordt verkregen of afgedwongen.

Toelichting

Persoonsgegevens die in het buitenland zijn meegenomen, bijvoorbeeld op een meegenomen laptop of elektronische toegang tot persoonsgegevens, kan leiden tot een vergrote kans op een datalek.

Persoonsgegevens doorgeven vanuit Nederland naar het buitenland mag daarom alleen als een land voldoende bescherming biedt. Voor doorgifte van gegevens naar een land binnen de Europese Unie (EU) gelden andere regels dan voor doorgifte naar een land buiten de EU. De EU is één rechtsgebied bij de bescherming van persoonsgegevens, omdat alle EU lidstaten zich moeten houden aan de AVG (GDPR). Voor doorgifte van persoonsgegevens van Nederland naar een ander EU-land moet alleen voldaan worden aan de algemene eisen uit de AVG.

Doelstelling	Het voorkomen van ongewenste toegang tot persoonsgegevens in het buitenland.		
Risico	Het ontstaan van een datalek, doordat in het buitenland een buitenlandse overheid, al dan niet door de uitoefening van buitenlandse wetgeving, zich toegang verschaft tot persoonsgegevens.		
Control	De organisatie hanteert regels voor medewerkers en andere verwerkers, die buiten Nederland **persoonsgegevens** of **authenticatiemiddelen** (voor de toegang tot persoonsgegevens vanuit het buitenland) met zich meedragen of in hun bezit hebben, ongeacht of deze informatie versleuteld is.		AVG: art. 32
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Persoons-gegevens	1.	De regels voor medewerkers bij het reizen naar het buitenland, of zij die in het buitenland gestationeerd worden of zijn, omvatten minimaal de volgende onderwerpen: 1. criteria voor de bepaling van de relevantie van het beleid voor medewerkers; 2. te nemen maatregelen ter bescherming van persoonsgegevens, bij het reizen naar het buitenland voorafgaande en tijdens de reis, op plaats van bestemming, en terugkeer, voor medewerkers; 3. contactgegevens van relevante medewerkers en instanties bij een (potentiële) inbreuk op de vertrouwelijkheid van de persoonsgegevens.	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties Algemene Inlichtingen- en Veiligheidsdienst. (2010, januari). Brochure Spionage bij reizen naar het buitenland. https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2010/02/04/brochure-spionage-bij-reizen-naar-het-buitenland/spionagebijreizennaarhetbuitenland.pdf
Authenticatie-middelen	2.	Toegang tot de gegevensverwerking, bijvoorbeeld voor het beheer van de systemen, en de doorgifte beperkt zich tot landen, waarvan de zekerheid bestaat dat de uitoefening van buitenlandse wetgeving niet kan leiden tot privacyrisico's.	Doorgifte binnen en buiten de EU: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal/doorgifte-binnen-en-buiten-de-eu
Wie	Opdrachtgever en opdrachtnemer		
Wat	Proces		
Verificatie	Overleg bewijsstukken en/of verklaring		

3.8 TBV P.08 Beëindiging (verwerkers)overeenkomst

Definitie

De AVG stelt eisen aan de verwerkingsverantwoordelijke en verwerker. De verwerkingsverantwoordelijke blijft altijd verantwoordelijk voor de persoonsgegevens die verwerkt worden. Ook wanneer die verwerking uitbesteedt is aan/uitgevoerd wordt door een verwerker. De persoonsgegevens zijn immers met de verwerkingsverantwoordelijke gedeeld en niet met de verwerker.

Een verwerkingsverantwoordelijke en een verwerker moeten samen een verwerkersovereenkomst afsluiten. Met een verwerkersovereenkomst sluit de verwerkingsverantwoordelijke uit dat de andere partij de persoonsgegevens voor eigen doelen mag verwerken/gebruiken.

Toelichting

Dit object beschrijft de eisen die aan een verwerker worden gesteld bij de beëindiging van een (verwerkers)overeenkomst.

Doelstelling	Het veiligstellen van persoonsgegevens bij beëindiging van een (verwerkers)overeenkomst.		
Risico	Schending van de privacy van betrokkenen, waarvan de persoonsgegevens worden verwerkt, doordat de privacy van deze betrokkenen na beëindiging van een (verwerkers)overeenkomst niet wordt geborgd.		
Control	De verwerkingsverantwoordelijke legt in de (verwerkers) overeenkomst afspraken vast, met de persoon of partij die persoonsgegevens verwerkt, over het **verwijderen** of **overdragen** van persoonsgegevens bij beëindiging van de relatie; eventuele **derden** worden over de beëindiging geïnformeerd.		AVG: art.32, AP Werkende verwerkersovereen-komsten september 2019[3]: 4.3.6
Conformiteitsindicator			**Afgeleid/afkomstig van**
Verwijderen	1.	De (verwerkers)overeenkomst bevat een regeling hoe de verwerker bij en na beëindiging van de relatie de vertrouwelijkheid van de persoonsgegevens, inclusief alle bestaande kopieën, borgt.	AP Werkende verwerkers-overeenkomsten september 2019: 4.3.6
Overdragen	2.	De (verwerkers)overeenkomst bevat een regeling hoe de verwerker bij en na beëindiging van de relatie de vertrouwelijkheid van de persoonsgegevens, inclusief alle bestaande kopieën, door het overdragen borgt en in welke vorm zij worden overgedragen.	AP Werkende verwerkers-overeenkomsten september 2019: 4.3.6
Derden	3.	Verwerker stelt alle ingeschakelde derden in kennis van de beëindiging van de (verwerkers)overeenkomst dan wel een daartoe strekkend verzoek van de verwerkingsverantwoordelijke en zal waarborgen dat zij de bij hen aanwezige persoonsgegevens (laten) vernietigen.	AP Werkende verwerkers-overeenkomsten september 2019: 4.3.6
Wie	Opdrachtgever en opdrachtnemer		
Wat	Proces		
Verificatie	Overleg bewijsstukken en/of verklaring		

[3] https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_verwerkersovereenkomsten.pdf

4 Privacy-maatregelen Huisvesting IV

4.1 HVI P.01 Uitvallen van een dienst

Definitie

Bij huisvesting wordt gebruik gemaakt van diensten, zoals nutsvoorzieningen van derde partijen of de eigen voorzieningen. Voorbeelden van deze diensten zijn gas, water en elektriciteit, maar ook een eigen voorziening, zoals een backup-voorziening voor elektriciteit.

Toelichting

Uitval van deze diensten kan leiden tot uitval van beschermingsmaatregelen. Bij ontbreken van mitigerende maatregelen kan dit bijvoorbeeld leiden tot onbeschikbaarheid of corrupt raken van de gegevensverwerking, verlies van persoonsgegevens en tot uitval van afschermingsmaatregelen. Dit met kans op een datalek of tot andere gevolgen in de persoonlijke levenssfeer van de betrokkenen, waarvan de persoonsgegevens worden verwerkt.

Doelstelling	Het nemen van maatregelen om de gevolgen van het uitvallen van diensten te voorkomen.		
Risico	Een datalek of andere gevolgen voor betrokkenen, waarvan de persoonsgegevens worden verwerkt, bij uitval van een dienst.		
Control	De organisatie heeft **maatregelen** getroffen die voorkomen dat de uitval van een **dienst**, of dit nu een eigen dienst is of van een derde, leidt tot een datalek of andere **gevolgen** voor betrokkenen, waarvan de persoonsgegevens worden verwerkt, en heeft een **procedure** om de werking van de maatregel te evalueren.		AVG: art. 24, 32, 35 en 36
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Maatregelen	1.	De organisatie heeft passende maatregelen getroffen om de de kans op een datalek of andere gevolgen voor betrokkenen, waarvan de persoonsgegevens worden verwerkt, door uitval van diensten te voorkomen.	AVG: art. 25
Dienst	2.	De organisatie heeft een overzicht beschikbaar van diensten waarvan de organisatie gebruik maakt, voor het verzorgen van (een deel van) de dienstverlening die wordt aangeboden aan de opdrachtgever.	CIP-netwerk
Gevolgen	3.	De organisatie heeft een beoordeling uitgevoerd op de impact van de uitval van diensten waar de organisatie gebruik van maakt, op de kans op een datalek of andere gevolgen voor betrokkenen, waarvan de persoonsgegevens worden verwerkt.	AVG: art. 35
Procedure	4.	Er is een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking bij uitval van een dienst.	AVG: art. 32 lid 1d
Wie	Opdrachtnemer		

Wat	Proces
Verificatie	Overleg bewijsstukken en/of verklaring

5 Privacy-maatregelen Serverplatform

5.1 SVP P.01 Dataminimalisatie door serverplatforms

Definitie

Bij minimale gegevensverwerking, ook wel dataminimalisatie genoemd zijn de persoonsgegevens beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt, onnodige verwerking wordt voorkomen. Onder verwerking wordt overeenkomstig de AVG bedoeld iedere vorm van verwerking, dus ook de opslag en het transport, al dan niet binnen het eigen netwerk.

Toelichting

Onnodige verwerking in tijd (duur, niet langer dan nodig voor de continuïteit van de verwerking) en locaties (niet meer dan nodig voor de continuïteit van de verwerking).

Bij transport gaat het hier om het transport tussen servers en de systemen voor opslag.

Doelstelling	De configuratie van servers hanteert dataminimalisatie als uitgangspunt, zodat niet meer systemen worden ingezet en (kopieën van) gegevens worden opgeslagen dan noodzakelijk voor de (continuïteit) van de dienstverlening.		
Risico	Door het niet beperken van het aantal systemen voor verwerking, transport en opslag neemt de kans op een datalek toe en daarmee de kans op inbreuk op de privacy van betrokkenen, waarvan de persoonsgegevens worden verwerkt.		
Control	De organisatie behoort een **proces** te hebben ingericht en **afspraken** te hanteren, zodat bij de **configuratie** van (onderdelen van) serverplatforms de instellingen gebruiken, waarbij enkel de minimaal benodigde hoeveelheid persoonsgegevens wordt verwerkt en **verwijdering** van persoonsgegevens mogelijk is.		AVG: art. 6 lid 1
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
Proces	1.	Een proces voor het configureren van (onderdelen van) serverplatforms is ingericht, waarbij een minimale verwerking (inclusief opslag en transport) als uitgangspunt wordt gehanteerd, en enkel de minimaal benodigde hoeveelheid persoonsgegevens wordt verwerkt.	CIP-netwerk
Afspraken	2.	De deployment en exploitatie zelf zijn gebaseerd op afspraken over hoe bij en na beëindiging van een deel van de verwerking, de gehele verwerking en de relatie tussen opdrachtgever en opdrachtnemer, de vertrouwelijkheid van de persoonsgegevens, inclusief alle bestaande kopieën, door en na het verwijderen geborgd wordt.	AP Werkende verwerkers-overeenkomsten september 2019: 4.3.6
Configuratie	3.	Het deploymentmodel en de exploitatie zijn getoetst op het hanteren van het uitgangspunt dataminimalisatie.	CIP-netwerk

Verwijdering	4.	Bij verwijdering of verplaatsing van persoonsgegevens zijn deze gegevens onherstelbaar verwijderd op de locatie waar deze waren opgeslagen; de opdrachtnemer heeft de methodiek voor het onherstelbaar verwijderen van de persoonsgegevens beschreven.	ISO 27701 2019: 6.8.2.7
Wie	Opdrachtnemer		
Wat	Product		
Verificatie	Overleg bewijsstukken en/of verklaring		

5.2 SVP P.02 Scheiden door serverplatforms

Definitie

Bij de scheiding van persoonsgegevens is de verwerking, het transport en opslag van persoonsgegevens, waarbij de gegevens aan dezelfde persoon toebehoren of die afkomstig zijn van meerdere bronnen en een aparte doelstelling voor verwerking kennen, gescheiden.

Toelichting

Compartimentering wordt gerealiseerd door gebruik te maken van fysiek gescheiden systemen en door het toepassen van virtualisatietechnieken, zoals servervirtualisatie, VPN's en opslagvirtualisatie.

Doelstelling	De verwerking, het transport en de opslag van persoonsgegevens die aan dezelfde persoon toebehoren en afkomstig zijn van meerdere bronnen, dan wel een aparte doelstelling voor verwerking kennen, zijn gescheiden.		
Risico	Als persoonsgegevens gekoppeld worden, kunnen profielen van personen gemaakt worden die niet voldoen aan de eisen van doelbinding, waardoor de verwerking onrechtmatig is.		
Control	De organisatie heeft een **proces** ingericht, zodat bij de **configuratie** van (onderdelen van) serverplatforms de instellingen gebruikt worden, waarbij de scheiding van verwerkingen het uitgangspunt is.		NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'scheiden': https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
Proces	1.	Een proces voor het configureren van (onderdelen van) serverplatforms is ingericht, waarin het duidelijk wordt welke gescheiden verwerkingen er moeten zijn en de scheiding van persoonsgegevens, tijdens de verwerking (inclusief de opslag en het transport) als uitgangspunt wordt gehanteerd.	CIP-netwerk

Configuratie	2.	Het deploymentmodel en de exploitatie zijn getoetst op het hanteren van de scheiding. Deze wordt verkregen door de opslag, verwerkingen en distributie in aparte compartimenten, waarbij de koppeling van de compartimenten door configuratie of encryptie onmogelijk is gemaakt.	CIP-netwerk
Wie	Opdrachtnemer		
Wat	Product		
Verificatie	Overleg bewijsstukken en/of verklaring		

5.3 SVP P.03 Verbergen door serverplatforms

Definitie

Bij het verbergen van persoonsgegevens worden persoonsgegevens en hun onderlinge relaties aan het zicht onttrokken, waardoor mogelijk misbruik wordt voorkomen.

Toelichting

Het verbergen van persoonsgegevens is ook één van de methoden om scheiding van verwerkingen mogelijk te maken. Op deze manier wordt onrechtmatige inzage en verwerking van persoonsgegevens voorkomen voor daartoe niet-gerechtigden.

De basismaatregelen voor het bieden van scheiding zijn een fysieke scheiding en een logische scheiding, waarbij de toegang door respectievelijk een fysieke toegangsvoorziening en een logische toegangsvoorziening wordt geboden. Versleutelen van de informatie is inmiddels een passende maatregel als aanvulling op het bieden van een fysieke of logische scheiding, die niet meer mag ontbreken als basismaatregel.

Doelstelling	De verwerking, het transport en de opslag van persoonsgegevens zijn aan het zicht onttrokken voor degenen die hiertoe geen doelbinding hebben, zodat onrechtmatige verwerking wordt voorkomen.	
Risico	Het ontstaan van een datalek, doordat een onrechtmatig verwerking door anderen, dan degenen die een doelbinding hebben, mogelijk is.	
Control	De organisatie heeft een **proces** ingericht, zodat bij de **configuratie** van (onderdelen van) serverplatforms de instellingen gebruikt worden, waarbij de scheiding van verwerkingen het uitgangspunt is.	NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'verbergen': https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design
Conformiteitsindicator, nummer en maatregel		Afgeleid/afkomstig van

Proces	1.	Een proces voor het configureren van (onderdelen van) serverplatforms, inclusief de opslag en het transport, is ingericht, waarin het duidelijk wordt welke persoonsgegevens onderling verborgen moeten zijn.	CIP-netwerk
Configuratie	2.	Het deploymentmodel en de exploitatie zijn getoetst op het hanteren van het verbergen van persoonsgegevens tijdens de opslag en distributie, zodat onrechtmatige inzage of verwerking onmogelijk is gemaakt, waarbij het duidelijk is waar en hoe fysieke scheiding, logische scheiding en versleuteling als maatregel wordt ingezet.	CIP-netwerk
Wie	Opdrachtnemer		
Wat	Product		
Verificatie	Overleg bewijsstukken en/of verklaring		

6 Privacy-maatregelen Applicatieontwikkeling

6.1 APO P.01 Testdata

Definitie

Er zijn twee methoden om voor het testen van software persoonsgegevens kunstmatig te genereren namelijk pseudonimiseren en anonimiseren. Beiden kunnen veilig zijn, maar er is een wezenlijk verschil tussen de twee.

1. Pseudonimiseren:
   Bij pseudonimiseren worden persoonsgegevens versleuteld, waardoor niet meer te zien is om welke 'natuurlijke' persoon het gaat. De 'sleutel' die hiervoor wordt gebruikt wordt op een andere plaats bewaard en is alleen toegankelijk voor geautoriseerde personen. Hierdoor ontstaat een extra beveiligingslaag. Via die sleutel kunnen de gegevens indien nodig weer terug worden gehaald.
2. Anonimiseren:
   Bij Anonimiseren zijn de persoonsgegevens eveneens versleuteld, maar kunnen niet meer terug worden gehaald. De sleutel is vernietigd, er bestaat geen 'schaduwbestand' meer. Anonimiseren is dus onomkeerbaar en om deze reden vallen geanonimiseerde gegevens niet langer onder de AVG: het zijn geen tot natuurlijke personen herleidbare gegevens meer.

Toelichting

Er kan een noodzaak bestaan om met (‘life’) persoonsgegevens te testen, als dit of technisch of financieel noodzakelijk is. Dit geldt als onomstotelijk gebleken is dat onvoldoende gegarandeerd wordt dat het systeem of de aanpassing ervan werkt of dat de kosten van het testen via versleutelde of fictieve persoonsgegevens zo hoog zijn dat het inzetten van deze maatregelen niet verantwoord wordt geacht. Of dit zo is zal op basis van een risicoanalyse moeten worden besloten.

Alleen wanneer het niet mogelijk is testdata kunstmatig te genereren en het gebruik van fictieve data niet mogelijk is, is het mogelijk na vooraf gegeven toestemming van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, persoonsgegevens in te zetten. Dit vraagt dan wel om de vastlegging van de beargumenteerde keuze en het nemen van passende beveiligingsmaatregelen, zodat de verwerkingsverantwoordelijke zich kan verantwoorden.

Ook bij het gebruik van pseudonimiseren en anonimiseren zijn passende beveiligingsmaatregelen noodzakelijk, omdat het bekend worden van een sleutel of het gebruik van een schaduwbestand alsnog kan leiden tot een datalek.

Doelstelling	Het waarborgen dat persoonsgegevens niet als testdata worden gebruikt en voldoende beveiligd zijn om een inbreuk op de privacy van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, te voorkomen.
Risico	Productiedata kunnen onbedoeld in omloop komen en daarmee een datalek zijn.

Control	Waar mogelijk wordt als **testdata** gebruik gemaakt van kunstmatig gegenereerde persoonsgegevens of fictieve data, wanneer op basis van de resultaten van een **risicoanalyse** gebruik gemaakt wordt van persoonsgegevens, worden passende **maatregelen** ter bescherming van de persoonsgegevens **genomen**.		ISO 27701 2019: 6.11.3.1, NEN 7510 2017: 14.3.1, AVG: art. 4.2, 6, 15, 25.1 en 32
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
Testdata	1.	Waar mogelijk maakt de organisatie gebruik van kunstmatig gegenereerde persoonsgegevens of fictieve data voor testdoeleinden, waarvan zeker is dat deze niet alsnog, tot natuurlijk personen herleidbaar zijn.	AVG: art. 6
Risicoanalyse	3.	Het besluit te testen met ('life') persoonsgegevens is gebaseerd op een risicoanalyse.	Testen met Persoonsgegevens oktober 2020 [Versie 2.1] 5.3: https://www.cip-overheid.nl/media/1544/testen-met-persoonsgegevens-21.pdf
Maatregelen	2.	De maatregelen genomen ter bescherming van de persoonsgegevens in de testomgeving, zijn beschreven en beschikbaar voor relevante medewerkers.	ISO 27701 2019: 6.11.3.1
Genomen	4.	Indien de organisatie voor het testen gebruik maakt van bestaande persoonsgegevens, worden in de testomgeving minimaal dezelfde maatregelen genomen ter bescherming van de persoonsgegevens, als in de productieomgeving.	AVG: art. 32
Wie	Opdrachtnemer		
Wat	Proces		
Verificatie	Overleg bewijsstukken en/of verklaring		

7 Privacy-maatregelen Maatwerk of maatwerkpakket

7.1 SSD P.01 Privacy by Default binnen applicaties en SSDm P.01 Privacy by Default binnen mobile apps

Definitie

Gegevensbescherming door standaardinstellingen (Privacy by default) betekent dat de applicatie standaard zo is geprogrammeerd, dat de applicatie zo privacy-vriendelijk mogelijk is en dus alleen die persoonsgegevens worden verwerkt met een duidelijk omschreven doel en afgestemd met de betrokkene, waarvan de persoonsgegevens worden verwerkt. De privacy by default geldt voor:

a) De hoeveelheid verzamelde persoonsgegevens;
b) De mate waarin de persoonsgegevens worden verwerkt;
c) De termijn waarvoor de persoonsgegevens worden opgeslagen;
d) De toegankelijkheid van de persoonsgegevens.

Toelichting

Nadat de betrokkene, waarvan de persoonsgegevens worden verwerkt, is geïnformeerd, moet deze vrijelijk en ondubbelzinnig toestemming kunnen geven om persoonsgegevens te laten verwerken. Met ondubbelzinnig wordt bedoeld dat bewust (actief) toestemming moet worden gegeven.

Doelstelling	De betrokkene, waarvan de persoonsgegevens worden verwerkt, moet bewust toestemming geven voor een verwerking.		
Risico	Als er geen grondslag of toestemming is voor de verwerking, is de verwerking onrechtmatig en wordt niet voldaan aan de eisen van doelbinding.		
Control	De applicatie vraagt bij elke verzameling van persoonsgegevens **vrijelijk** en ondubbelzinnig **toestemming** aan betrokkene, waarvan de persoonsgegevens worden verwerkt, om de gegevens te mogen verwerken, waarbij **standaard** zo min mogelijk persoonsgegevens worden verwerkt.		CIP De Privacy Baseline 2020: U.05, AVG: art. 25
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
Vrijelijk	1.	Het niet of beperkt toestemmen om (aanvullende) persoonsgegevens te verwerken gaat niet ten koste van de standaard functionaliteit van de applicatie.	AVG: art. 14 lid 4
Toestemming	2.	Het verzoek om toestemming te geven om de gegevens te verwerken is goed leesbaar en begrijpelijk voor 'de gewone burger'.	AVG: art. 7 lid 2

Standaard	3.	De applicatie heeft als standaardinstelling de keuze, waarbij zo min mogelijk informatie over de (potentiële) betrokkene, waarvan de persoonsgegevens worden verwerkt, wordt verzamelt en verwerkt, zodat deze keuze minder tijd en interactie vraagt, dan de keuze voor instellingen waarbij meer informatie wordt verzameld.	AVG: art. 14 lid 4
Wie	Opdrachtnemer		
Wat	Product		
Verificatie	Testen		

7.2 SSD P.02 Correcte en gewenste verwerking met applicaties en SSDm P.02 Correcte en gewenste verwerking met mobile apps

Definitie

Een correcte verwerking van persoonsgegevens is alleen mogelijk, wanneer maatregelen zijn getroffen die, bij onjuistheid en onnauwkeurigheid van de persoonsgegevens, de mogelijkheid bieden om de gegevens te rectificeren, volledig te maken, te wissen of bij ongewenste verwerking, de verwerking te beperken of te beëindigen.

Toelichting

Persoonsgegevens kunnen op verzoek van betrokkene, waarvan de persoonsgegevens worden verwerkt, worden gerectificeerd, vervolledigd of gewist als dit op (volgens AVG) gegronde redenen gebeurt.

Doelstelling	Een gegevensverwerking die correct en volgens de wens van betrokkene, waarvan de persoonsgegevens worden verwerkt, is.	
Risico	Wanneer de gegevens onjuist of onnauwkeurig zijn ingevoerd of gecorrumpeerd raken, worden verkeerde conclusies over de betrokkene, waarvan de persoonsgegevens worden verwerkt, getrokken wat negatieve consequenties tot gevolg kan hebben of naar het oordeel van deze betrokkene ongewenste verwerking van zijn of haar persoonsgegevens.	
Control	De applicatie biedt de mogelijkheid om **op aangeven van betrokkene**, waarvan de persoonsgegevens worden verwerkt, controle te houden over de gegevens en de verwerking ervan, zodat de **juistheid en nauwkeurigheid** van de gegevens kan worden gewaarborgd en de verwerking ervan kan worden **gecorrigeerd, gestaakt of overgedragen**.	AVG: art. 7, 11, 12, 16, 17, 18, 19, 20, 21, 22 en 23
Conformiteitsindicator, nummer en maatregel		Afgeleid/afkomstig van

Op aangeven van betrokkene	1.	Er is een proces beschreven en ingeregeld, zodat op aangeven van de betrokkene, waarvan de persoonsgegevens worden verwerkt, de persoonsgegevens worden gecontroleerd op juistheid, actualiteit en nauwkeurigheid en zo nodig gecorrigeerd of overgedragen kunnen worden of dat de verwerking wordt gestaakt.	CIP De Privacy Baseline 2020: B.01/02.04, AVG: art. 5 lid 1d
Juistheid en nauwkeurig-heid	2.	Binnen de applicatie zijn de nodige maatregelen, inclusief periodieke controles, getroffen om de juistheid en nauwkeurigheid van persoonsgegevens te waarborgen en zo nodig te verbeteren.	CIP De Privacy Baseline 2020: U.03/01.01
Gecorrigeerd, gestaakt of overgedragen	3.	Op verzoek van betrokkene, waarvan de persoonsgegevens worden verwerkt, moeten zijn of haar persoonsgegevens kunnen worden gerectificeerd, vervolledigd, gewist of in bruikbare vorm worden overgedragen, of moet de verwerking ervan kunnen worden beperkt of gestaakt.	AVG: art. 16, 20 en 21
Wie	Opdrachtnemer		
Wat	Product		
Verificatie	Overleg bewijsstukken en/of verklaring en testen		

7.3 SSD P.03 Informatieverstrekking aan betrokkene met applicaties en SSDm P.03 Informatieverstrekking aan betrokkene met mobile apps

Definitie

Wie persoonsgegevens verstrekt aan een organisatie heeft het recht te weten waarvoor, op welke wijze en door wie deze gegevens worden gebruikt. De organisatie heeft hiertoe een informatieplicht. Deze informatieplicht geldt ook wanneer persoonsgegevens van anderen worden ontvangen.

Toelichting

In de AVG is vastgelegd welke informatie moet worden verstrekt bij ontvangst van een verzoek van de betrokkene, waarvan de persoonsgegevens worden verzameld, en welke informatie moet worden verstrekt bij ontvangst van een verzoek van een ander dan deze betrokkene (AVG art. 13).

Doelstelling	Het is voor betrokkene, waarvan de persoonsgegevens worden verwerkt, transparant hoe de persoonsgegevens worden verzameld en verwerkt.
Risico	De organisatie is niet transparant, waardoor de organisatie niet kan verantwoorden dat de gegevensverwerking voldoet aan de beginselen van behoorlijke en transparante verwerking, met mogelijk hoge kosten tot gevolg.

Control	Om de gegevens te mogen verwerken wordt de betrokkene, waarvan de persoonsgegevens worden verwerkt, **geïnformeerd** betreffende welke verwerking (van de persoonsgegevens) plaatsvindt en krijgt deze betrokkene een **waarschuwing** bij het verkrijgen van toegang tot bijzondere persoonsgegevens.		CIP De Privacy Baseline 2020: U.05, AVG: art. 14 en overweging 60
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
Geïnformeerd	1.	De organisatie heeft een proces ingericht, zodat duidelijk is wanneer het verstrekken van informatie wettelijk vereist is, wanneer een uitzondering geldt en welke informatie verstrekt moet worden.	AVG: art. 14
Waarschu-wing	2.	De applicatie geeft een waarschuwing aan gebruikers bij het verkrijgen van toegang tot bijzondere persoonsgegevens, over het belang van de vertrouwelijkheid van de bijzondere persoonsgegevens die de applicatie verwerkt.	NEN 7510 2017: A.8.2.2
Wie	Opdrachtgever en opdrachtnemer		
Wat	Product		
Verificatie	Testen		

7.4 SSD P.04 Toegang op taakniveau tot applicaties en SSDm P.04 Toegang op taakniveau tot mobile apps

Definitie

Dit object beschrijft de eisen die aan de toegang tot verwerkingen en daarmee ook tot applicaties worden gesteld, waarbij de toegang gespecificeerd wordt tot op taakniveau. Een verwerking mag immers alleen plaatsvinden voor een specifiek doel, ofwel een specifieke taak. Het is daarmee een aanvulling op de toegang op basis van rollen.

De toegang op basis van rollen wordt doorgaans in een toegangsbeveiligingssysteem bijgehouden. Doordat doelbinding een taakgebonden karakter heeft en het taakgebonden karakter tijdsgebonden is, kan dit niet ondersteund worden vanuit een toegangsbeveiligingssysteem maar zal de toegang op taakniveau binnen de applicatie geregeld moeten worden.

Taken worden vaak toegekend op basis van het behandelen van een dossier. In dat geval spreekt men ook wel van dossiergebonden toegang.

Toelichting

Hoe toegangsbeveiliging op basis van rollen plaatsvindt is bij de Privacy-maatregelen voor Toegangsbeveiliging beschreven. De toegang op basis van rollen is niet fijnmazig en slechts beperkt tijdsgebonden. De op basis van rollen, uitgegeven toegangsrechten geven daardoor ook toegang tot persoonsgegevens die voor het op dat moment geldende doel niet gerechtvaardigd zijn. Door toegang taakgebonden en daarmee ook meer tijdsgebonden te maken, dan het geval is als dit op basis van rollen gebeurt, wordt de toegang steeds specifiek voor één verwerkingsdoel verstrekt.

Het tijdsgebonden karakter van toegang op taakniveau vraagt om het toekennen van toegangsrechten op taakniveau binnen de applicatie. Welke toegangsrechten binnen de applicatie worden beheerd en welke binnen een (centraal) autorisatiesystemen, wordt bepaald tijdens de ontwikkeling van de applicatie.

Doelstelling	Het verstrekken van toegang tot persoonsgegevens, waarvan de toegang is gebaseerd op rechtvaardige gronden, die tijdsgebonden zijn.		
Risico	De toegang op basis van rollen is niet fijnmazig en slechts beperkt tijdsgebonden, waardoor de uitgegeven toegangsrechten op basis van rollen ook toegang geven tot persoonsgegevens die voor het op dat moment geldende doel niet gerechtvaardigd zijn, waardoor voor een verwerking geen rechtmatige grond bestaat en hierdoor wordt niet voldaan aan de eisen van doelbinding.		
Control	Het verlenen van toegang tot persoonsgegevens wordt **beperkt** op basis van duidelijke en afgebakende **taken** en het doel en de verstrekte toegang is **toetsbaar**.		CIP-netwerk
Conformiteitsindicator			Afgeleid/afkomstig van
Beperkt	1.	De taken zijn zodanig vastgesteld dat zij het fijnmazig en tijdsgebonden toestaan van de toegang mogelijk maken, zodat een verwerker geen persoonsgegevens kan inzien die niet nodig zijn voor het uitvoeren van zijn (op dat moment toegewezen) taak en persoonsgegevens niet kunnen worden gekoppeld waardoor ongewenste profilering mogelijk is.	ENISA strategie (January 12, 2015) 'minimalisatie': https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design, BIO Thema-uitwerking Toegangsbeveiliging 2020: U.07
Taken	2.	De rechten die zijn beperkt op basis van taken worden beheerd binnen de applicatie.	CIP-netwerk
Toetsbaar	3.	Het doel en het verstrekken van de toegang is zodanig vastgelegd (welbepaald) dat het een kader biedt waaraan getoetst kan worden of de toegang noodzakelijk is.	AVG: art. 6 lid 4
Wie	Opdrachtnemer		
Wat	Product		
Verificatie	Overleg bewijsstukken en/of verklaring		

7.5 SSD P.05 Logging binnen applicaties en SSDm P.05 Logging binnen mobile apps

Definitie

Logging is bij het beheren van de toegang tot persoonsgegevens een methode voor het bijhouden en opslaan van informatie over bijvoorbeeld wie toegang heeft gehad en wanneer. Gedurende het monitoren wordt beoordeeld of de toegang rechtmatig was en dus aan de doelbindingseisen heeft voldaan.

Toelichting

In de te ontwikkelen verwerkingssystemen moeten faciliteiten voor logging en monitoring zijn ingebouwd die ertoe bijdragen dat rechtmatige en onrechtmatige pogingen om persoonsgegevens te in te zien of te wijzigen gedetecteerd en vastgelegd kunnen worden. Doordat de toegang door verwerkers, zoals medewerkers, veelal via een applicatie verloopt is dit de aangewezen plek de toegang te loggen.

Doelstelling	Onrechtmatige pogingen om persoonsgegevens in te zien of te wijzigen worden tijdig gedetecteerd en vastgelegd, zodat via de logregistratie de oorzaak van een datalek kan worden achterhaald of daar een bijdrage aan kan leveren en dat onrechtmatige pogingen worden ontmoedigd of zelfs voorkomen.		
Risico	Het niet kunnen signalen van onrechtmatige pogingen om toegang te krijgen vergroot de kans op datalekken, dan wel maakt het moeilijk om de oorzaak/veroorzaker van een datalek te achterhalen.		
Control	De applicatie behoort op verwerkers/persoonsniveau te **loggen**, zodat direct of **periodiek** kan worden **beoordeeld** welke persoonsgegevens deze medewerker heeft opgevraagd, ingezien en aangepast.		AVG: art. 5 lid 2 en art. 33 lid 5
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
Loggen	1.	De applicaties, waarin persoonsgegevens worden verwerkt of toegankelijk zijn, houden een logregistratie bij, waarin op persoonsniveau geregistreerd is op welk tijdstip/wie toegang had tot deze persoonsgegevens.	CIP-netwerk
Periodiek	2.	Voor de gelogde gegevens is een bewaartermijn vastgesteld.	CIP De Privacy Baseline 2020: Privacyprincipe Doelbinding U.01
Beoordeeld	3.	De logbestanden worden gedurende een overeengekomen periode bewaard voor toekomstig onderzoek en toegangscontrole.	CIP-netwerk
Wie	Opdrachtnemer		
Wat	Product		
Verificatie	Overleg bewijsstukken en/of verklaring		

7.6 SSD P.06 Dataminimalisatie binnen applicaties en SSDm P.06 Dataminimalisatie binnen mobile apps

Definitie

Bij minimale gegevensverwerking, ook wel dataminimalisatie genoemd zijn de persoonsgegevens beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt, onnodige verwerking in tijd en locaties wordt voorkomen. Onder verwerking wordt overeenkomstig de AVG bedoelt iedere vorm van verwerking, dus ook de opslag en het transport, al dan niet binnen het eigen netwerk.

Toelichting

Het aantonen van het op de juiste wijze bereiken van dataminimalisatie is mogelijk door het uitvoeren van een daarop gerichte analyse, het formeel en beheersbaar vastleggen van de resultaten en het hanteren van passende technieken.

Doelstelling	De applicatie is gebouwd met dataminimalisatie als uitgangspunt, zodat niet meer persoonsgegevens worden verwerkt en niet meer verwerking plaatsvindt dan noodzakelijk voor de het uitvoeren van de dienstverlening.		
Risico	Door het niet beperken van de verwerking en het aantal persoonsgegevens neemt de kans op een datalek toe en daarmee de kans op inbreuk op de privacy van betrokkenen, waarvan de persoonsgegevens worden verwerkt.		
Control	De organisatie behoort een **proces** te hebben ingericht, waarbinnen een **analyse** wordt gemaakt en **aantoonbaar** is dat het verzamelen van de persoonsgegevens rechtmatig en noodzakelijk is en het ontwerp getoetst wordt aan het **uitgangspunt dataminimalisatie**, de juiste **wijze van opslag** en het hanteren van de **bewaartermijn**.		AVG: art. 6 lid 1
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
Proces	1.	De organisatie behoort een proces te hebben ingericht, zodat gewaarborgd is dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en dat de gegevens niet op een met die doeleinden onverenigbare wijze worden verwerkt.	CIP De Privacy Baseline 2020: B.01/02.02, AVG: art. 6 lid 1
Analyse	2.	Een analyse is gemaakt, zodat van ieder persoonsgegeven aantoonbaar is dat het in relatie staat tot het doel en dat het doel niet met minder gegevens kan worden bereikt.	CIP De Privacy Baseline 2020: 3.1.2

Aantoonbaar	3.	De applicatie hanteert metagegevens, zodat gegevens als doelbinding en bewaartermijn als verantwoording beschikbaar zijn voor controledoeleinden en de metagegevens worden samen met de persoonsgegevens opgenomen in het verwerkingsregister.	UC Berkeley School of Information. (z.d.). Sticky Policies - Privacy Patterns. privacypatterns. https://privacypatterns.org/patterns/Sticky-policy, CIP De Privacy Baseline 2020: 3.1.2
Uitgangspunt dataminimali-satie	4.	Het ontwerp is getoetst op het hanteren van het uitgangspunt dataminimalisatie.	CIP-netwerk
Wijze van opslag	5.	Beschreven is hoe gewaarborgd wordt dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor de verwerking en in welke vorm de opslag moet plaatsvinden, zodat na deze periode de betrokkenen, waarvan de persoonsgegevens worden verwerkt, niet langer zijn te identificeren.	CIP De Privacy Baseline 2020: B.01/02.07
Bewaartermijn	6.	Persoonsgegevens worden door de applicatie geautomatiseerd verwijderd, na het verstrijken van de bewaartermijn die gekoppeld is aan persoonsgegevens, hiertoe kan binnen de applicatie de bewaartermijnen aan persoonsgegevens worden meegegeven.	CIP-netwerk
Wie	Opdrachtgever en opdrachtnemer		
Wat	Product		
Verificatie	Overleg bewijsstukken en/of verklaring		

7.7 SSD P.07 Generalisatie binnen applicaties en SSDm P.07 Generalisatie binnen mobile apps

Definitie

Bij het generaliseren van persoonsgegevens wordt het persoonsgegeven vervangen door een meer generieke aanduiding. Zo kan een leeftijd van 35 jaar vervangen worden door een leeftijdsaanduiding van 30-40 jaar. Generalisatie vindt plaats in 2 stappen. In de eerste stap (de 'aggregatie') wordt het gegeven geaggregeerd naar een gegeven dat voor een grotere groep geldt en in de tweede stap wordt bekeken hoeveel keer de gegevens binnen de gegeneraliseerde groep voorkomt (de controle op 'diversiteit'). Als de gegeneraliseerde groep te klein is en de persoon, waar een gegeneraliseerd gegeven vandaan komt is te achterhalen (bijvoorbeeld door correlatie met andere gegeneraliseerde gegevens), dan moet de groep groter gemaakt worden.

Door generalisatie is het persoonsgegeven zo geanonimiseerd dat het gegeven nog wel bruikbaar blijft voor het doel waarvoor het is verzameld.

Toelichting

Het generaliseren van een gegeven gebeurt direct na ontvangst, waarbij het ontvangen gegeven niet wordt bewaard.

Doelstelling	Het voorkomen dat een persoonsgegeven onnodig persoonsgebonden is en misbruik van het gegeven onnodig mogelijk is.		
Risico	Een persoonsgegeven is onnodig persoonsgebonden, waardoor kans op inbreuk op de privacy van betrokkenen bestaat.		
Control	De applicatie behoort, indien de **functionele eisen** aan de applicatie van de opdrachtgever dit toelaten, **gegeneraliseerde gegevens** te **gebruiken**.		ENISA strategie (January 12, 2015) 'generaliseren': https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Functionele eisen	1.	De organisatie heeft de mogelijkheden tot het omzetten van persoonsgegevens naar gegeneraliseerde gegevens, op basis van de functionele eisen van de opdrachtgever aan de applicatie, vastgesteld.	CIP-netwerk
Gegenerali-seerde gegevens	2.	Persoonsgegevens zijn na ontvangst gegeneraliseerd, zodat herleiding naar de persoon met dit (en andere gegevens) niet mogelijk is.	CIP-netwerk
Gebruiken	3.	De applicatie gebruikt bij verdere verwerking, enkel de generalisatie van de ontvangen persoonsgegevens	CIP-netwerk
Wie	Opdrachtnemer		
Wat	Product		
Verificatie	Overleg bewijsstukken en/of verklaring		

7.8 SSD P.08 Scheiden binnen applicaties en SSDm P.08 Scheiden binnen mobile apps

Definitie

Bij de scheiding van persoonsgegevens is de verwerking, het transport en de opslag van persoonsgegevens, waarbij de gegevens aan dezelfde persoon toebehoren of die afkomstig zijn van meerdere bronnen en een aparte doelstelling voor verwerking kennen, gescheiden.

Toelichting

De scheiding moet en kan op de verschillende onderdelen van de applicatie worden gerealiseerd. Het is daarom van belang de maatregelen los van elkaar en in samenhang te bekijken, zodat de scheiding effectief én efficiënt is.

Doelstelling	De applicatie, het transport en de opslag van persoonsgegevens die aan dezelfde persoon toebehoren en die afkomstig zijn van meerdere bronnen, dan wel een aparte doelstelling voor verwerking kennen, zijn gescheiden.		
Risico	Als persoonsgegevens gekoppeld worden, kunnen profielen van personen gemaakt worden die niet voldoen aan de eisen van doelbinding, waardoor de verwerking onrechtmatig is.		
Control	Iedere applicatie kent een duidelijk **verwerkingsdoel**, waarbij de scheiding van de verwerking gerealiseerd is op het niveau van de **applicatie**, de **transportpaden**, de **middleware,** de **opslagvoorzieningen** en is hierop **getoetst**.		AVG: art. 6 lid 1, ENISA strategie (January 12, 2015) 'scheiden': https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Verwerkings-doel	1.	Iedere applicatie heeft een duidelijk beschreven verwerkingsdoel, zodat duidelijk is welke gescheiden verwerkingen er moeten zijn. De scheiding van persoonsgegevens, tijdens de verwerking (inclusief de opslag en het transport) moet als uitgangspunt worden gehanteerd. De verwerkingsdoelen zijn opgenomen in het verwerkingsregister.	AVG: art. 6 lid 1, CIP-netwerk
Applicatie	2.	Iedere (runtime omgeving van een) applicatie heeft zijn eigen verwerkingsdoel. Koppelingen met andere verwerkingen zijn alleen mogelijk, wanneer deze in het verwerkingsregister zijn opgenomen.	CIP-netwerk
Transport-paden	3.	Transportpaden binnen de verwerking zijn gescheiden van die van de omgeving en andere verwerkingen.	CIP-netwerk
Middleware	4.	Middleware oplossingen, zoals Enterprise Service Bussen (ESB), databases en e-mail, zijn zo ingericht dat de scheiding van persoonsgegevens met een verschillend verwerkingsdoel als uitgangspunt wordt gehanteerd.	CIP-netwerk
Opslag-voorzieningen	5.	De opslag van persoonsgegevens is zo ingericht dat persoonsgegevens met een verschillend verwerkingsdoel zijn gescheiden als deze scheiding niet in de middleware kan worden gegarandeerd.	CIP-netwerk
Getoetst	6.	Het implementatiemodel is getoetst op het hanteren de scheiding.	CIP-netwerk
Wie	Opdrachtnemer		
Wat	Product		
Verificatie	Overleg bewijsstukken en/of verklaring		

7.9 SSD P.09 Verbergen binnen applicaties en SSDm P.09 Verbergen binnen mobile apps

Definitie

Bij het verbergen van persoonsgegevens worden persoonsgegevens en hun onderlinge relaties aan het zicht onttrokken, waardoor mogelijk misbruik wordt voorkomen. Het verbergen van de informatie is mogelijk door het niet onnodig tonen van de informatie en door het versleutelen van de informatie.

Toelichting

Door het verbergen van persoonsgegevens wordt onrechtmatige inzage en verwerking van persoonsgegevens voorkomen door daartoe niet-gerechtigden.

Om aan de eis van scheiding te voldoen ontvangt en heeft een applicatie toegang tot alleen die informatie die noodzakelijk is voor het uitvoeren van zijn taak. Het opvragen of tonen van een verzameling van gegevens, waarvan slechts een deel noodzakelijk voor het uitvoeren van een taak, voldoet daarmee niet aan de eis van verbergen.

Versleutelen van de informatie is inmiddels een passende maatregel, als aanvulling op het selectief tonen of doorgeven, die niet meer mag ontbreken als basismaatregel. Door bij het versleutelen van de persoonsgegevens de sleutel per verwerkingsdoel te variëren, wordt onderlinge toegang of inzage voorkomen.

Doelstelling	De verwerking, het transport en de opslag van persoonsgegevens zijn aan het zicht onttrokken voor degenen die hiertoe geen doelbinding hebben, zodat een onrechtmatige verwerking door anderen wordt voorkomen.		
Risico	Het ontstaan van een datalek, doordat een onrechtmatig verwerking door anderen, dan degenen die een doelbinding hebben, mogelijk is.		
Control	Een **applicatie,** en iedere **Functie** binnen deze applicatie, heeft een duidelijk omschreven verwerkingsdoel, zodat bij iedere **doorgifte**, **verwerking door de applicatie** en **verwerking binnen een functie** alleen de daarvoor noodzakelijke persoonsgegevens worden doorgegeven of zijn in te zien, waarbij de andere persoonsgegevens verborgen blijven door het toepassen van versleuteling van de **opslagvoorzieningen**, de **transportpaden** en de **middleware**. Het implementatiemodel is **getoetst**.		NEN 7510 2017: A.12.3.1**,** ENISA strategie (January 12, 2015) 'verbergen': https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Applicatie	1.	Iedere applicatie heeft een duidelijk beschreven verwerkingsdoel, zodat het duidelijk is welke informatie noodzakelijk is tijdens de verwerking (inclusief de opslag en het transport). De verwerkingsdoelen en de gebruikte informatie zijn opgenomen in het verwerkingsregister.	AVG: art. 6 lid 1, CIP-netwerk
Functie	2.	Iedere functie binnen de applicatie heeft een duidelijk beschreven verwerkingsdoel, zodat het duidelijk is welke informatie noodzakelijk is voor het uitvoeren van die functie. De verwerkingsdoelen zijn duidelijk omschreven.	CIP-netwerk

Doorgifte	3.	Bij de doorgifte van gegevens worden alleen die gegevens doorgegeven die noodzakelijk zijn voor het vooraf vastgelegde doel van de doorgifte.	CIP-netwerk
Verwerking door de applicatie	4.	Iedere (runtimeomgeving van een) applicatie heeft zijn eigen verwerkingsdoel. Vanuit de applicatie is toegang/inzage tot alleen die informatie die noodzakelijk is voor het uitvoeren van de verwerking door die applicatie toegestaan.	CIP-netwerk
Verwerking binnen een functie	5.	Iedere functie binnen de applicatie heeft zijn eigen verwerkingsdoel. Vanuit die functie is toegang/inzage tot alleen die informatie toegestaan die noodzakelijk is voor het uitvoeren van die functie.	CIP-netwerk
Opslag-voorzieningen	6.	De opslag van persoonsgegevens is zo ingericht dat alleen die informatie is ontsleuteld die noodzakelijk is voor de werking van de applicatie.	CIP-netwerk
Transport-paden	7.	Transportpaden binnen de verwerking zijn versleuteld, tenzij op basis van een analyse is gebleken dat scheiding een afdoende maatregel is.	CIP-netwerk
Middleware	8.	Middleware oplossingen, zoals ESB, databases en e-mails, zijn zo ingericht dat inzage of toegang wordt voorkomen door het versleutelen van de persoonsgegevens, waarbij de sleutel verschilt per verwerkingsdoel, zodat gegevens onderling verborgen zijn.	CIP-netwerk
Getoetst	9.	Het implementatiemodel is getoetst op het hanteren van het principe van verbergen, zodat zeker is dat de persoonsgegevens en hun onderlinge relaties aan het zicht zijn onttrokken.	CIP-netwerk
Wie	Opdrachtnemer		
Wat	Product		
Verificatie	Overleg bewijsstukken en/of verklaring		

8 Privacy-maatregelen Communicatievoorzieningen

8.1 CVZ P.01 Scheiden binnen communicatievoorzieningen

Definitie

Bij het gebruik van persoonsgegevens is de verwerking, het transport en de opslag van persoonsgegevens, waarbij de gegevens aan dezelfde persoon toebehoren of die afkomstig zijn van meerdere bronnen en een aparte doelstelling voor verwerking kennen, gescheiden.

Toelichting

Compartimentering wordt mogelijk gemaakt door gebruik te maken van fysiek gescheiden systemen en door het toepassen van virtualisatietechnieken, zoals servervirtualisatie, VPN's en opslagvirtualisatie.

Doelstelling	Het transport van persoonsgegevens die aan dezelfde persoon toebehoren en die afkomstig zijn van meerdere bronnen, dan wel een aparte doelstelling voor verwerking kennen, zijn gescheiden.		
Risico	Als persoonsgegevens gekoppeld worden, kunnen profielen van personen gemaakt worden die niet voldoen aan de eisen van doelbinding, waardoor de verwerking onrechtmatig is.		
Control	De organisatie heeft een **proces** ingericht, zodat bij de **configuratie** van (onderdelen van) het netwerk de instellingen gebruikt worden, waarbij de scheiding van verwerkingen het uitgangspunt is.		NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'scheiden': https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
Proces	1.	Een proces voor het configureren van (onderdelen van) het netwerk is ingericht, waarbij het duidelijk wordt welke gescheiden verwerkingen er moeten zijn en waarbij de scheiding van persoonsgegevens, tijdens het transport als uitgangspunt wordt gehanteerd.	CIP-netwerk
Configuratie	2.	Het deployment model en de exploitatie zijn getoetst op hoe het hanteren van de scheiding wordt verkregen door het transport in aparte compartimenten, waarbij de koppeling van de compartimenten door configuratie of encryptie onmogelijk is gemaakt.	CIP-netwerk
Wie	Opdrachtnemer		
Wat	Product		
Verificatie	Overleg bewijsstukken en/of verklaring		

8.2 CVZ P.02 Verbergen binnen communicatievoorzieningen

Definitie

Bij het verbergen van persoonsgegevens worden deze en hun onderlinge relaties aan het zicht onttrokken, waardoor mogelijk misbruik wordt voorkomen.

Toelichting

Het verbergen van persoonsgegevens is ook één van de methoden om scheiding van verwerkingen mogelijk te maken. Op deze manier wordt onrechtmatige inzage en verwerking van persoonsgegevens voorkomen door daartoe niet-gerechtigden.

De basismaatregelen voor het bieden van scheiding zijn een fysieke scheiding en een logische scheiding. Versleutelen van de informatie is inmiddels een passende maatregel als aanvulling op het bieden van een fysieke en/of logische scheiding, die niet meer mag ontbreken als basismaatregel.

Doelstelling	De verwerking, het transport en de opslag van persoonsgegevens zijn aan het zicht onttrokken voor degenen die hiertoe geen doelbinding hebben, zodat een onrechtmatige verwerking door onbevoegden wordt voorkomen.		
Risico	Het ontstaan van een datalek doordat een onrechtmatige verwerking door anderen, dan degenen die een doelbinding hebben, mogelijk is.		
Control	De organisatie heeft een **proces** ingericht, zodat bij de **configuratie** van (onderdelen van) het netwerk de instellingen gebruikt wordt, waarbij het verbergen van verwerkingen het uitgangspunt is.		NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'verbergen': https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
Proces	1.	Een proces voor het configureren van (onderdelen van) serverplatforms (inclusief de opslag en het transport) is ingericht, waarin duidelijk wordt welke persoonsgegevens onderling verborgen moeten zijn.	CIP-netwerk
Configuratie	2.	Het deploymentmodel en de exploitatie zijn getoetst op hoe het hanteren van het verbergen van persoonsgegevens tijdens het transport geregeld is, zodat onrechtmatige inzage of verwerking onmogelijk is gemaakt, waarbij het duidelijk is waar en hoe fysieke scheiding, logische scheiding en versleuteling als maatregel wordt ingezet.	CIP-netwerk
Wie	Opdrachtnemer		
Wat	Product		
Verificatie	Overleg bewijsstukken en/of verklaring		

8.3 CVZ P.03 Logging binnen communicatievoorzieningen

Definitie

Logging is bij het beheren van de toegang tot persoonsgegevens een methode voor het bijhouden en opslaan van informatie over bijvoorbeeld wie toegang heeft gehad en wanneer. Gedurende het monitoren wordt beoordeeld of de toegang rechtmatig was en dus aan de doelbindingseisen voldaan is.

Toelichting

In de te ontwikkelen verwerkingssystemen moeten faciliteiten voor logging en monitoring zijn ingebouwd die ertoe bijdragen dat alle pogingen om persoonsgegevens in te zien of te wijzigen gedetecteerd en vastgelegd worden.

Doelstelling	Onrechtmatige pogingen om op het netwerk persoonsgegevens in te zien of te wijzigen worden tijdig gedetecteerd en vastgelegd, doordat in de logregistratie de oorzaak van een datalek kan worden achterhaald of dat daar een bijdrage aan kan worden geleverd en onrechtmatige pogingen worden ontmoedigd of zelfs voorkomen.		
Risico	Het niet kunnen signalen van onrechtmatige pogingen om toegang te krijgen vergroot de kans op datalekken, dan wel maakt het moeilijk om de oorzaak/veroorzaker van een datalek te achterhalen.		
Control	De logging en monitoring van het netwerk behoort op verwerkers/persoonsniveau te **loggen**, zodat direct of **periodiek** kan worden **beoordeeld** welke persoonsgegevens deze medewerker heeft opgevraagd, ingezien en aangepast.		AVG: art. 5 lid 2 en art. 33 lid 5
Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
Loggen	1.	De verwerkingen, waarin persoonsgegevens worden gebruikt, houden een logregistratie bij, waarin op persoonsniveau duidelijk is op welk tijdstip wie toegang had tot deze persoonsgegevens.	CIP-netwerk
Periodiek	2.	Voor de gelogde gegevens is een bewaartermijn vastgesteld.	CIP De Privacy Baseline 2020: Privacyprincipe Doelbinding:
Beoordeeld	3.	De logbestanden worden gedurende een overeengekomen periode bewaard voor toekomstig onderzoek en toegangscontrole.	CIP- netwerk
Wie	Opdrachtgever en opdrachtnemer		
Wat	Product		
Verificatie	Overleg bewijsstukken en/of verklaring		

9 Privacy-maatregelen Clouddiensten

9.1 Samenvoeging van eisen

Voor clouddiensten gelden alle eisen van Hoofdstuk 2 tot en met 8!!