Privacy Control Framework

Rapportage Self Assessment

Ten behoeve van: Test Bedrijf

Inhoudsopgave

Klantgegevens	
Bedrijfsnaam	Test Bedrijf
Naam	Test Tester
Functie	Functionaris Gegevensbescherming Testbedrijf
E-mail	joost@itriskcontrol.nl
Object van onderzoek	Test Bedrijf
Invul datum	24/5/2019

Inleiding

Het Privacy Control Framework (in het Nederlands "Handreiking") wordt uitgegeven door NOREA, de beroepsvereniging van IT-auditors in Nederland. Voor meer informatie zie Norea.

Het Privacy Control Framework biedt geschikte criteria voor Nederlandse IT-auditors (Register IT auditors, RE's) om hen te begeleiden bij het uitbrengen van privacycontrolerapporten in het kader van de EU-algemene verordening gegevensbescherming (GDPR) en de internationale normen voor betrouwbaarheidsverklaringen (ISAE).

Doelstellingen van het Privacy Control Framework

Het primaire doel van het Privacy Control Framework, hierna PCF, is begeleiding te bieden aan (audit) professionals bij het beoordelen of de beheersdoelstellingen van een entiteit inzake privacy en de bescherming van persoonsgegevens worden bereikt. Het PCF kan daarbij worden gebruikt als startpunt voor op maat gemaakte privacy-audits. Het PCF bevat de voorgeschreven besturingsdoelen en illustratieve bedieningselementen voor privacy-opdrachten op basis van de Assurance 3000-norm ('NOREA Richtlijn 3000).

Daarnaast kan het PCF worden ingezet om de adequaatheid van privacy maatregelen te beoordelen of om de hiaten te bepalen tussen de huidige staat van maatregelen en de ambities in het licht van (veranderende) wetgevende kaders (bijvoorbeeld de AVG).

Gebruik van het Privacy Control Framework

Het gebruik in de praktijk is afhankelijk van de doelstellingen van de gebruiker. Over het algemeen worden drie soorten gebruikers onderscheiden:

1. Een IT-auditor die de privacy maatregelen van een entiteit en het behalen van privacy doelstellingen beoordeelt, met als doel bijvoorbeeld te pogen de privacy-gereedheid of GDPR-nauwkeurigheid te beoordelen;
2. Een IT-auditor die een privacy assurance-opdracht uitvoert op basis van standaard 3000 ('NOREA Richtlijn 3000') (attest (A) of directe rapportage (D));
3. Andere professionals (zoals risicomanagers, gegevensbeschermings-, beveiligings- en privacyfunctionarissen) die streven naar het beoordelen van privacy volwassenheid of GDPR-gereedheid (niet-audit) in een entiteit.

Het PCF kan als startpunt dienen om de privacy onderwerpen en bijbehorende beheersdoelstellingen vast te stellen die zo goed mogelijk aansluiten bij de doelstellingen van een onderzoek. Als tweede stap kan dan worden bepaalde welke beheersmaatregelen moeten worden geëvalueerd.

In het geval van assurance opdrachten kan het PCF als basis dienen voor criteria die kunnen worden opgenomen in assurance-rapporten volgens de 3000-norm ('NOREA Richtlijn 3000'). Bij het uitvoeren van de assurance opdracht kan de IT-auditor de onderwerpen integreren en beheersingsdoelstellingen opnemen/vermelden in het normenkader in het assurance-rapport.

Het PCF maakt geen expliciet onderscheid tussen de doelstellingen van de privacy- maatregelen die moeten worden gerealiseerd door de verantwoordelijke en die moeten worden bereikt door de verwerker(s). Het feit dat (een deel van) een beoordeelde entiteit duidelijk kan worden gekarakteriseerd als - bijvoorbeeld - alleen een verwerker, kan een reden zijn om sommige van de maatregelen buiten de reikwijdte van het onderzoek te laten.

Online Assessment

Om de toepassing van Privacy Control Framework te vergroten en het gebruik te vergemakkelijken is een online assessment ontwikkeld. Het assessment faciliteert een gestructureerde selectie en inventarisatie van relevante beheersdoelstellingen en de beoordeling van de status van de daarmee samenhangende beheersmaatregelen.

Deze rapportage bevat de uitkomsten van een online assessment dat is uitgevoerd op basis van het Privacy Control Framework.

De uitkomsten geven een gestructureerd en concreet inzicht in de status van beheersmaatregelen, mogelijke \risico's en maken het mogelijk, waar nodig, gericht actie te kunnen ondernemen.

Disclaimer

Het PCF is bedoeld te helpen bij het beoordelen van een kader voor privacy beheers raamwerk. Elk resultaat, score of aanbeveling tot stand gekomen op basis van de toepassing van het PCF, mag niet op zichzelf worden gebruikt om te bepalen hoe de GDPR van toepassing is op een entiteit en/of de beoordeling van de naleving door een entiteit van GDPR. Het PCF vormt geen juridisch advies, certificering of garantie met betrekking tot het nakomen van de GDPR.

De rol van het online assessment en deze rapportage is gericht op het faciliteren van het proces om op een doelmatige en doeltreffende wijze inzicht te krijgen en beperkt zich tot het systematisch verzamelen en structureren van informatie en het inzichtelijk maken van een aantal mogelijke relevante aandachtspunten. Een validatie van de antwoorden maakt geen onderdeel uit van het online assessment en/of deze rapportage.

Uitkomsten Online Assessment

In het navolgende zijn de uitkomsten van het online assessment opgenomen. Dit betreft de;

I Managementsamenvatting,
II Detail bevindingen.

Daarnaast zijn drie bijlagen opgenomen. Het betreft;

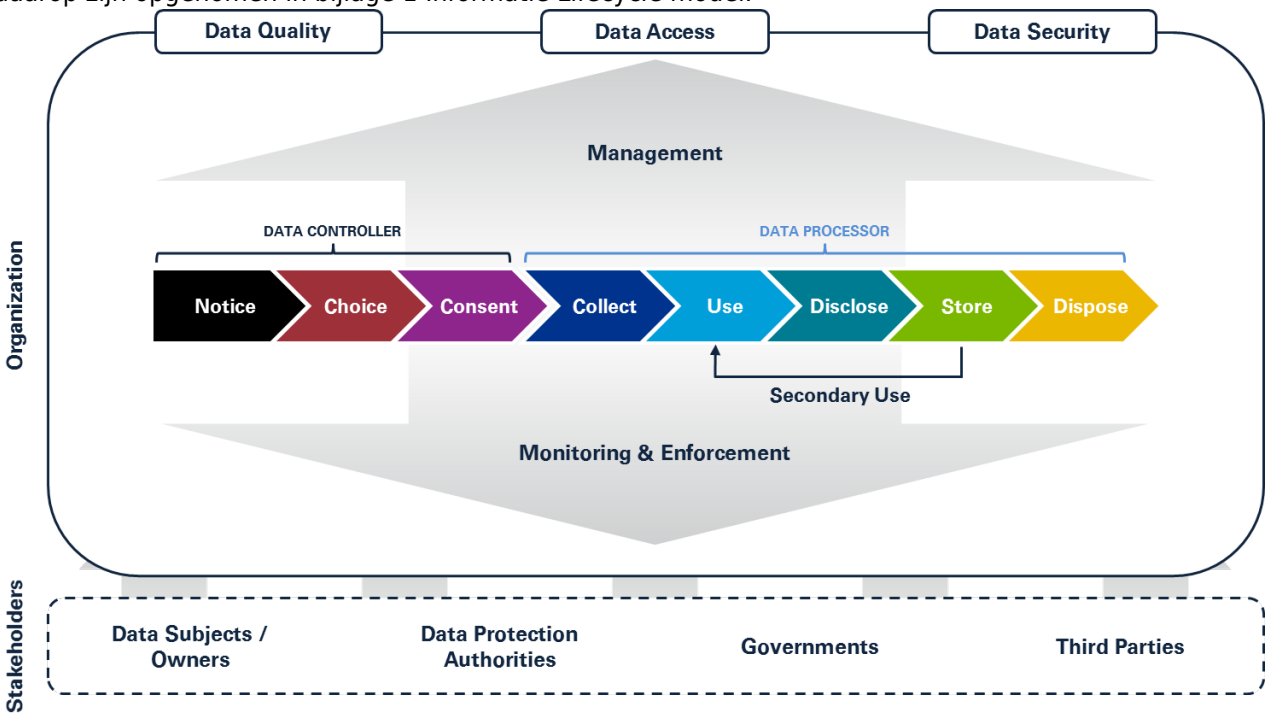
Bijlage 1: Informatie Lifecycle model,
Bijlage 2: Uitkomsten assessment per beheersdoelstelling,
Bijlage 3: Cross referentie tussen GDPR key elementen en GDPR artikelen.

Management samenvatting

Dit hoofdstuk bevat de managementsamenvatting. Het geeft op hoofdlijn inzicht in de uitkomsten van het online assessment.

Structuur Privacy Control Framework

Het framework is gestructureerd volgens een Information Lifecycle-model. Dit model en een toelichting daarop zijn opgenomen in bijlage 1 Informatie Lifecycle model.



Beheersdoelstellingen

Voor elke fase in het model zijn toepasselijke privacyonderwerpen vastgesteld. Dit betreft:

- Beheer
- Kennisgeving
- Keuze en Toestemming
- Verzamelen
- Gebruik, bewaren en verwijderen
- Gegevenstoegang en -kwaliteit
- Openbaren
- Data beveiliging
- Monitoring en handhaving

Per privacy onderwerp zijn een of meerdere beheersdoelstellingen geformuleerd, in totaal 32. Een beheersdoelstelling kan worden geoperationaliseerd door maatregelen. In totaal zijn 104 maatregelen geformuleerd.

Resultaten assessment

In het assessment is gevraagd de privacy-onderwerpen en beheersdoelstellingen te selecteren, die voor het betreffende onderzoek relevant zijn. Van deze selectie is vervolgens gevraagd aan te geven in welke

mate in de samenhangende beheersmaatregelen is voorzien.

Onderwerp	**#**	**Antwoorden**					
		Voldoen helemaal	Voldoen grotendeels	Voldoen deels	Voldoen niet	N.v.t.	N/I
Beheer	42	4	24	6	8	0	0
Kennisgeving	2	1	1	0	0	0	0
Keuze en toestemming	4	1	3	0	0	0	0
Verzamelen	2	1	0	1	0	0	0
Gebruik, bewaren en verwijderen	12	5	3	4	0	0	0
Data toegang en data kwaliteit	18	14	3	1	0	0	0
Openbaren	4	1	3	0	0	0	2
Databeveiliging	10	1	6	2	1	0	4
Monitoring en handhaving	4	0	0	3	0	0	1
Totalen	105	**28**	**43**	**17**	**9**	**0**	**7**

Tabel: Uitkomsten per cyclus

Een gedetailleerd overzicht per maatregel, is opgenomen in bijlage 3: Uitkomsten assessment per beheersdoelstelling.

De relevantie van de privacy-onderwerpen, beheersdoelstellingen varieert per entiteit. Dit geldt ook voor de beheersmaatregelen en de wijze waarop en mate waarin daaraan wordt of moet worden voldaan. Belangrijke aspecten zijn bijvoorbeeld de aard van de persoonsgegevens en de eisen die daarbij aan de verantwoordelijke en/of verwerkers worden gesteld. Situaties zijn zelden gelijk. Daarom is het niet mogelijk om aan de uitkomsten van het online assessment een eenduidige en absolute conclusie te verbinden.

De uitkomsten geven inzicht in de privacy-onderwerpen die voor de entiteit als toepasselijk zijn aangemerkt. De scores op de onderliggende beheersdoelstellingen en -maatregelen per privacy onderwerp geven aan waar niet/ niet geheel wordt voldaan. Deze scores kunnen worden gebruikt om gericht in te zoomen en waar nodig aanvullende maatregelen te treffen.

Daar waar wordt voldaan kunnen de uitkomsten worden gebruikt om de toepasselijkheid van de privacy-onderwerpen te toetsen en een nadere toetsing op de effectieve werking van de maatregelen uit te (laten)voeren.

Verdere aanpak

Op basis van de uitkomsten kan een overwogen beslissing worden genomen voor de verdere aanpak en het al dan niet instellen van nader (professioneel) onderzoek, indien de uitkomsten van het assessment

daartoe aanleiding geven. Het is de verantwoordelijkheid van de gebruiker van dit rapport, om afgestemd op de doelstellingen van het assessment, de adequaatheid van het rapport en de uitkomsten te beoordelen en op basis daarvan de hiaten te bepalen tussen de huidige staat van maatregelen en de ambities van de entiteit.

De rol van het online assessment en deze rapportage beperkt tot het systematisch verzamelen en structureren van informatie en het inzichtelijk maken van een aantal mogelijke relevante aandachtspunten. Een validatie van de antwoorden maakt geen onderdeel uit van het online assessment.
Op basis van de uitkomsten kan een overwogen beslissing worden genomen voor de verdere aanpak en het al dan niet instellen van nader (professioneel) onderzoek, indien de uitkomsten van het assessment daartoe aanleiding geven.
Het is de verantwoordelijkheid van de gebruiker van dit rapport, om afgestemd op de doelstellingen van het assessment, de adequaatheid van het rapport en de uitkomsten te beoordelen en op basis daarvan de hiaten te bepalen tussen de huidige staat van maatregelen en de ambities van de entiteit.

Detailbevindingen

Dit hoofdstuk geeft de detailbevindingen van het online assessment weer. Voor elk van de 9 privacy onderwerpen worden de details gerapporteerd volgens de volgende structuur:

- Naam Privacy onderwerp:
  - Een overzicht van de beheersdoelstellingen;
  - Per beheersdoelstelling:
    - De beschrijving van de doelstelling;
    - De maatregelen voor het realiseren van de beheersdoelstelling;
    - De antwoorden op de vraag of wordt voldaan aan de beheersmaatregel. Opties zijn:
      - Voldoet/voldoen helemaal
      - Voldoet/voldoen grotendeels
      - Voldoet/voldoen deels
      - Voldoet/voldoen niet
    - Als een maatregel niet relevant is de mogelijkheid geboden om ‘n.v.t.’ aan te geven.
    - Een toelichting en/of aanvullende opmerkingen te geven als daarvan gebruik is gemaakt. Als geen gebruik is gemaakt van deze mogelijkheid is het tekstvak voorzien van de tekst '*Geen aanvullende opmerkingen*'.
- Aan het einde van elk privacy onderwerp een verwijzing naar relevante GDPR elementen.

Beheer

Dit privacy-onderwerp betreft de volgende beheersdoelstellingen:

- Privacybeleid (PPO)
- Definitie van rollen en verantwoordelijkheden (RRE)
- Identificatie en classificatie van persoonlijke gegevens (PDI)
- Risk Management (RMA)
- Gegevensbeschermingseffectrapportages (PIA)
- Privacy Incident en Breach Management (PIB)
- Personeelsbevoegdheden (SCO)
- Bewustwording en training van personeel (SAT)
- Juridische beoordeling van wijzigingen in wettelijke en / of zakelijke vereisten (LRC)

Een beheersdoelstelling kan worden geoperationaliseerd door een of meerdere maatregelen. In het assessment is gevraagd aan te geven in welke mate in de betreffende beheersmaatregelen is voorzien. Daarbij zijn de volgende antwoorden verkregen.

Privacy beleid (PPO)

De entiteit heeft een beleid vastgesteld en gecommuniceerd waarin de doelstellingen en verantwoordelijkheden met betrekking tot privacy zijn bepaald en dat in overeenstemming is met de aanvaarde privacybeginselen en toepasselijke wet- en regelgeving.

Beheersmaatregel	**Antwoord**
PPO01: Er is een gedocumenteerd privacybeleid, dat is gecommuniceerd met intern personeel en externe belanghebbenden, dat is vastgesteld en dat jaarlijks door het management wordt beoordeeld en goedgekeurd.	Grotendeels
PPO02: Het management erkent nadrukkelijk haar verantwoordelijkheid en committeert zich aan deugdelijke en wettige privacyprincipes.	Grotendeels
PPO03: Het privacybeleid vermeldt de doelstellingen van de entiteit met betrekking tot privacy en bescherming van persoonsgegevens.	Grotendeels
PPO04: Voor elke verwerking van persoonsgegevens zorgt de entiteit dat deze in lijn is met de aanvaarde en wettelijke privacyprincipes en documenteert de wijze waarop de naleving van deze principes wordt gerealiseerd.	Helemaal
PPO05: Voor elk geval van verwerking heeft de entiteit criteria opgesteld en gedocumenteerd op basis waarvan de wettige verwerking van persoonsgegevens wordt gegarandeerd en aangetoond.	Grotendeels

Toelichting bij deze beheersdoelstelling:
Beleid is vastgesteld en wordt jaarlijks gereviewed.

GDPR Elementen	Privacybeginselen art 5 Rechtmatigheid van verwerking art 6 Registratie van verwerkingsactiviteiten art 30

Definitie van rollen en verantwoordelijkheden (RRE)

De entiteit heeft eenduidige rollen en verantwoordelijkheden vastgesteld en geïmplementeerd met betrekking tot het waarborgen van persoonsgegevens en het bereiken van de privacydoelstellingen.

Beheersmaatregel	Antwoord
RRE01: Voor elk geval van verwerking van persoonsgegevens heeft de entiteit vastgesteld en gedocumenteerd of de entiteit fungeert als verantwoordelijke óf verwerker.	Helemaal
RRE02: In geval de entiteit als een verwerker opereert zijn er overeenkomsten met de verantwoordelijke waarin de privacy verantwoordelijkheden van de verwerker zijn geregeld.	Helemaal
RRE03: In geval de entiteit als verantwoordelijke fungeert, zijn er overeenkomsten met verwerkers welke de privacyverantwoordelijkheden van de verwerker bepalen. Als de entiteit als een gezamenlijke verantwoordelijke fungeert, is een overeenkomst met de andere verantwoordelijken aanwezig.	Grotendeels
RRE04: De entiteit wijst de coördinatie, toezicht en monitoring van privacy toe aan een specifiek persoon zoals een privacy officer of een functionaris voor gegevensbescherming (DPO). De verantwoordelijkheid, het gezag en de verantwoordelijkheid van de persoon zijn duidelijk gedocumenteerd en worden regelmatig beoordeeld.	Grotendeels
RRE05: De rollen en verantwoordelijkheden van individuele medewerkers bij het beschermen van persoonsgegevens en de naleving van privacyprincipes zijn vastgesteld en gecommuniceerd.	Deels

Toelichting bij deze beheersdoelstelling:
Communicatie naar individuele gebruikers kan veel beter

GDPR Elementen	Privacybeginselen art 5 Verantwoordelijkheden van verantwoordelijke en verwerker, art 24,28 Registratie van verwerkingsactiviteiten art 30 Functionaris voor gegevensbescherming (DPO), art 27-39 Overdracht van persoonsgegevens aan derde landen of internationale organisaties, art 44-50

Identificatie en classificatie van persoonlijke gegevens (PDI)

De entiteit begrijpt en documenteert welke persoonsgegevens worden opgeslagen, verwerkt en identificeert en behandelt persoonsgegevens op de juiste manier. Maatregelen om persoonsgegevens te beschermen houden rekening met de verschillen in gevoeligheid in de persoonsgegevens en leidt tot identificatie van risico's en naleving van wet- en regelgeving.

Beheersmaatregel	Antwoord
PDI01: De entiteit implementeert een beheerst en gedocumenteerd proces om de verwerking van persoonsgegevens te identificeren, te documenteren en de gegevens als zodanig te classificeren. Dit omvat mede processen, systemen en derde partijen welke persoonsgegevens verwerken.	Grotendeels
PDI02: De entiteit onderscheidt en documenteert duidelijk verwerkingsgevallen van: 1. persoonsgegevens en 2. bijzondere categorieën van persoonsgegevens.	Grotendeels
PDI03: De entiteit past een procedure toe om te beoordelen of bestaande of geplande verwerking van persoonsgegevens bijzondere categorieën vanpersoonsgegevens omvat. Als dit het geval is, wordt expliciet de rechtmatigheid van de (geplande) verwerking nagegaan en gedocumenteerd en worden passende maatregelen getroffen om een veilige en compliant verwerking te garanderen.	Grotendeels

PDI04: De entiteit onderhoudt en beheert een systematisch overzicht van activiteiten aangaande de verwerking van persoonsgegevens, met inbegrip van de kenmerken van deze activiteiten (legitieme basis, doel, gegevenscategorieën en betrokkenen, ontvangers).	Grotendeels

Toelichting bij deze beheersdoelstelling:
Er is geen gebruik gemaakt van de mogelijkheid om een toelichting te geven bij deze beheersdoelstelling.

GDPR Elementen	Privacybeginselen art 5 Registratie van verwerkingsactiviteiten art 30 Beveiliging van de verwerking, art 32

Risk Management (RMA)

De entiteit identificeert, evalueert en mitigeert systematisch en periodiek de factoren die het behalen van privacydoelstellingen in gevaar brengen.

Beheersmaatregel	**Antwoord**
RMA01: Er is een proces voor het periodiek identificeren van gebeurtenissen welke de privacydoelstellingen in gevaar brengen.	Niet
RMA02: Er is een proces om de impact en de waarschijnlijkheid van dergelijke gebeurtenissen periodiek te beoordelen en vervolgens adequate risicoreacties en beheersmaatregelen te formuleren.	Grotendeels
RMA03: Als nieuwe of gewijzigde privacy risico‘s worden vastgesteld, worden de risicobeoordeling van het privacyrisico en de risicoreactiestrategieën geëvalueerd en waar nodig bijgewerkt.	Deels
RMA04: Criteria voor acceptatie van privacy risico‘s worden goedgekeurd, gedocumenteerd en toegepast.	Niet
RMA05: De entiteit plant en implementeert de interne beheersingsmaatregelen welke nodig zijn om het privacyrisico te mitigeren. De voortgang van de implementatie wordt gemonitord en gemeten.	Deels

Toelichting bij deze beheersdoelstelling:
Risico/management is op dit moment onvoldoende ingebed in de organisatie

GDPR Elementen	Privacy by Design/ by Default, art 25 Gegevensbescherming Impact Assessment (DPIA), art 35

Gegevensbeschermingseffectrapportages (DPIA)

De privacy-gerelateerde impact van nieuwe producten en diensten en het gebruik ervan binnen de entiteit wordt systematisch geïdentificeerd, beoordeeld en opgepakt.

Beheersmaatregel	**Antwoord**
PIA01: De entiteit implementeert een beheerst en gedocumenteerd proces voor het beoordelen van de impact op de privacy bij nieuwe of aanzienlijk gewijzigde processen, producten en diensten.	Grotendeels

PIA02: In de beoordeling wordt rekening gehouden met de risico‘s voor de privacy van de betrokkene als gevolg van de beoogde wijzigingen en de maatregelen om deze risico‘s te beperken.	Grotendeels
PIA03: In de beoordeling wordt rekening gehouden met de doeleinden van de verwerking in relatie tot de noodzaak en proportionaliteit van de verwerking van de persoonsgegevens.	Grotendeels
PIA04: Het proces zorgt ervoor dat alle relevante belanghebbenden bij de beoordeling worden betrokken en dat specifieke richtlijnen van de toezichthoudende autoriteit betreffende beoordelingscriteria worden nageleefd.	Grotendeels
PIA05: De entiteit documenteert alle systemen en software welke persoonsgegevens verwerken en houdt een overzicht bij van wijzigingen welke daarop zijn toegepast.	Grotendeels
PIA06: Het wijzigingsbeheerproces van de entiteit zorgt ervoor dat goedgekeurde privacy maatregelen (vanuit de beoordeling) zijn geïmplementeerd vóórdat de wijziging wordt doorgevoerd.	Deels

Toelichting bij deze beheersdoelstelling:
Vaak zijn zaken al Live alvorens de maatregelen zijn geìmplementeerd

GDPR Elementen	Privacy by Design/ by Default, art 25 Gegevensbescherming Impact Assessment (DPIA), art 35

Privacy Incident en Breach Management (PIB)

De entiteit detecteert en behandelt privacygerelateerde incidenten adequaat; privacygerelateerde incidenten worden op gepaste wijze beantwoord om de gevolgen te beperken en maatregelen te nemen om toekomstige inbreuken te voorkomen.

Beheersmaatregel	**Antwoord**
PIB01: Een formeel, allesomvattend privacy-incident en inbreukbeheer proces is geïmplementeerd en omvat: 1. De verantwoordelijkheid van medewerkers om de verantwoordelijke privacy officer te informeren in geval van een privacy incident of een mogelijke schending van gegevens 2. De privacy officer (of, indien van toepassing, security officer) beoordeelt of het incident privacy gerelateerd is. In het geval van inbreuk op persoonsgegevens , documenteert de privacy officer de aard van de overtreding, de gevolgen en het geschatte aantal gegevensrecords en de gegevens onderwerpen welke het betreft. 3. De privacy officer initieert en coördineert de vereiste acties, bepaalt de vereiste betrokkenheid van individuen en belanghebbenden welke moeten worden geïnformeerd (zoals de verantwoordelijke in het geval dat de entiteit een verwerker is). 4. De privacy officer houdt toezicht op de voortgang van de herstelacties en rapporteert aan het management (en indien van toepassing, informeert de verantwoordelijke).	Helemaal
PIB02: De privacy officer heeft de algehele verantwoordelijkheid voor het (management)proces inzake schendingen.Incidenten en inbreuken welke geen persoonsgegevens inhouden, zijn de verantwoordelijkheid van de security officer.	Grotendeels
PIB03: Het proces bevat een duidelijk escalatiepad, gebaseerd op het type of ernst, of beide, van het incident, met inbegrip van het inwinnen van juridisch advies en het betrekken van C-level management. Het proces houdt rekening met de criteria voor het opnemen van contact met de wet handhavings-, regelgevende - of andere autoriteiten.	Grotendeels

PIB04: De entiteit heeft een meldingsbeleid voor schending van de privacywetgeving dat waarborgt dat de toezichthoudende autoriteit tijdig op de hoogte wordt gebracht van een datalek als de inbreuk waarschijnlijk resulteert in een risico voor de rechten en vrijheden van natuurlijke personen.	Grotendeels
PIB05: Het proces waarborgt dat alle vereiste informatie over de inbreuk wordt verzameld en aan de toezichthoudende autoriteit wordt verstrekt, inclusief mitigerende maatregelen.	Grotendeels
PIB06: De privacy officer heeft de algehele verantwoordelijkheid voor het proces van kennisgeving van inbreuken. De privacyfunctionaris documenteert alle overwegingen welke worden gemaakt bij het bepalen of de meldingsplicht van toepassing is.	Grotendeels
PIB07: Het proces voor het beheer van inbreuken omvat mede en schetst dat lesssons learned van inbreuken leiden tot remedies en verbeteringen en dienen als input voor bewustmakings- programma's voor privacy bewustzijnsprogramma's voor het personeel.	Niet
PIB08: Het proces voor privacy incidenten en inbreuken omvat mede het volgende: 1. na een groot privacy incident of datalek wordt een formele evaluatie van het incident uitgevoerd, waar nodig met externe expertise 2. periodiek wordt een beoordeling van actuele incidenten uitgevoerd en worden noodzakelijke verbeteringen geïdentificeerd op basis van het volgende 3. de oorzaakanalyse van incidenten 4. incidentpatronen 5. veranderingen in de interne beheersing- omgeving en wet-/regelgeving 6. resultaten van de periodieke beoordeling en voortgang van verbeteringen worden gerapporteerd aan en beoordeeld door het management	Grotendeels
PIB09: Het proces voor het beheer van inbreuken wordt minstens elk jaar herzien en direct na de implementatie van een belangrijk systeem of procedurele wijzigingen.	Niet

Toelichting bij deze beheersdoelstelling:
Is nu vrij statisch proces, mede omdat het nog niet is voorgekomen

GDPR Elementen	Persoonlijke gegevens inbreuk, art 33, 34

Personeelsbevoegdheden (SCO)

Medewerkers in functies met toegang tot of controle over persoonsgegevens en persoonsgegevensprocessen hebben de noodzakelijke privacycompetenties om hun taken adequaat te kunnen uitvoeren.

Beheersmaatregel	**Antwoord**
SCO01: De entiteit heeft de vereiste competenties voor medewerkers welke betrokken zijn bij het omgaan met persoonsgegevens gedocumenteerd en geformaliseerd. Tevens is vastgesteld hoe deze competenties kunnen worden bereikt (bijvoorbeeld door trainingsprogramma's).	Grotendeels
SCO02: De entiteit documenteert de mate waarin individuele personeelsleden over deze competenties bezitten. Er is een proces om hiaten in de competenties te overbruggen.	Niet
SCO03: De entiteit betrekt privacy competenties bij het aannemen van personeel/inhuur en betrekt de naleving van privacy door betrokkenen bij individuele beoordelingen.	Deels
SCO04: Management beoordeelt jaarlijks de toewijzing van personeel, budgetten en andere middelen voor haar privacy programma.	Deels

Toelichting bij deze beheersdoelstelling:
Is niet echt standaard ingebed bij Personeelsprocessen

GDPR Elementen	Privacybeginselen art 5 Beveiliging van de verwerking, art 32 Functionaris voor gegevensbescherming (DPO), art 27-39

Bewustwording en training van personeel (SAT)

Het personeel is voldoende op de hoogte van privacywetten, voorschriften, organisatorische privacybeleidslijnen, -richtlijnen en hun individuele verantwoordelijkheden met betrekking tot privacy. De entiteit biedt programma's om het bewustzijn te creëren en te onderhouden.

Beheersmaatregel	Antwoord
SAT01: Om het privacybeleid van de entiteit en de implicaties ervan te begrijpen worden: • Voor alle werknemers minstens een keer per jaar een cursus over privacy- en veiligheidsbewustzijn georganiseerd • Nieuwe werknemers, aannemers en anderen verplicht om binnen een maand na aanvang een vergelijkbare opleiding te voltooien.	Niet
SAT02: Op basis van de noodzakelijke privacy competenties van het personeel (zie Personeelsbevoegdheden) wordt een diepgaande (interne of externe) privacy training aangeboden.De training omvat privacy en relevant beveiligingsbeleid en -procedures, overwegingen inzake weten regelgeving, incidentrespons en gerelateerde onderwerpen. Een dergelijke training is: • jaarlijks verplicht voor alle werknemers met toegang tot persoonsgegevens of verantwoordelijk voor de bescherming van persoonsgegevens Voor alle werknemers minstens een keer per jaar een cursus over privacy- en veiligheidsbewustzijn georganiseerd • afgestemd op de verantwoordelijkheden van de werknemer en de vereiste competenties.	Niet
SAT03: Trainingen- en bewustwordingscursussen worden beoordeeld en geactualiseerd aan vereisten vanuit wetgeving, regelgeving-, industrie en het beleid en de procedures van de entiteit.	Niet

Toelichting bij deze beheersdoelstelling:
Dit is nu niet georganiseerd, is eenmalig gedaan, niet periodiek aandacht voor

GDPR Elementen	Privacybeginselen art 5 Beveiliging van de verwerking, art 32

Juridische beoordeling van wijzigingen in wettelijke en / of zakelijke vereisten(LRC)

Privacyrisico's die verband houden met veranderingen in de entiteit (structuur en strategie) en wettelijke vereisten worden adquaat in overweging genomen.

Beheersmaatregel	Antwoord

LRC01: De entiteit implementeert een proces om de impact op privacy vereisten te bewaken, te beoordelen en aanpassingen door te voeren bij veranderingen door: 1. wet- en regelgeving 2. branchevereisten, best practices en richtlijnen 3. contracten, inclusief service-level-agreements met derden (wijzigingen in de privacy- en beveiligingsgerelateerde clausules in contracten worden adequaat beoordeeld en goedgekeurd voordat ze deze worden doorgevoerd) 4. bedrijfsactiviteiten en processen 5. in personen welke verantwoordelijk zijn voor privacy- en beveiligingsaangelegenheden 6. technologie (voorafgaand aan de implementatie).	Grotendeels

Toelichting bij deze beheersdoelstelling:
Er is geen gebruik gemaakt van de mogelijkheid om een toelichting te geven bij deze beheersdoelstelling.

GDPR Elementen	Rechtmatigheid van verwerking art 6 Gegevensbescherming Impact Assessment (DPIA), art 35

Kennisgeving

Dit privacy-onderwerp betreft de volgende beheersdoelstelling:

- Privacyverklaring (PST)

Een beheersdoelstelling kan worden geoperationaliseerd door een of meerdere maatregelen. In het assessment is gevraagd aan te geven in welke mate in de betreffende beheersmaatregelen is voorzien. Daarbij zijn de volgende antwoorden verkregen.

Privacyverklaring (PST)

De entiteit informeert de betrokkenen op transparante wijze over het beleid, de vereisten en de handelswijze van de entiteit met betrekking tot het verzamelen, gebruiken, bewaren, openbaar maken en verwijderen van persoonsgegevens.

Beheersmaatregel	Antwoord
DPST01: De privacyverklaring van de entiteit: 1. beschrijft de verkregen persoonsgegevens, de bronnen daarvan, de doeleinden waarvoor zij worden verzameld en de toepasselijke rechtmatigheidscriteria 2. beschrijft de eventuele gevolgen voor de betrokkene als de gevraagde gegevens niet worden verstrekt 3. beschrijft (indien van toepassing) de verdere verwerking)	Helemaal
PST02: De privacyverklaring is: 1. gemakkelijk beschikbaar en toegankelijk voor betrokkenen op het moment dat persoonsgegevens voor het eerst worden verzameld bij de betrokkene 2. tijdig aangeboden (dat wil zeggen, op of voor het tijdstip) dat de persoonsgegevens worden verzameld, of zo snel als praktisch daarna mogelijk, om betrokkenen te kunnen laten beslissen al dan niet persoonlijke gegevens beschikbaar te stellen aan de entiteit 3. duidelijk gedateerd, zodat betrokkenen kunnen bepalen of de privacy verklaring is veranderd sinds de laatste keer dat zij deze hebben gelezen of sinds de vorige keer dat zij persoonsgegevens aan de entiteit beschikbaar hebben gesteld.	Grotendeels

Toelichting bij deze beheersdoelstelling:
Is duidelijk en goed toegankelijk voor iedereen

GDPR Elementen	Privacybeginselen art 5 Privacybeginselen art 5 Rechten van de betrokkene, art 12-19 Verantwoordelijkheden van verantwoordelijke en verwerker, art 24,28

Keuze en toestemming

Dit privacy-onderwerp betreft de volgende beheersdoelstelling:

- Toestemmingskader (CFR)

Een beheersdoelstelling kan worden geoperationaliseerd door een of meerdere maatregelen. In het assessment is gevraagd aan te geven in welke mate in de betreffende beheersmaatregelen is voorzien. Daarbij zijn de volgende antwoorden verkregen.

Toestemmingskader (CFR)

De entiteit verkrijgt de toestemming van de betrokkene voor het verwerken van persoonsgegevens wanneer dit nodig of noodzakelijk is.

Beheersmaatregel	Antwoord
CFR01: De privacyverklaring van de entiteit beschrijft duidelijk en kernachtig het volgende: 1. de keuzes voor de persoon met betrekking tot de verzameling, het gebruik en het openbaren van persoonsgegevens 2. het proces dat een persoon moet volgen om deze keuzes uit te oefenen (door bijvoorbeeld een opt-outvakje aan te vinken om de ontvangst te weigeren van marketingmateriaal) 3. de mogelijkheid en het proces voor de persoon om de contactvoorkeuren te veranderen 4. de gevolgen van het niet verstrekken van de vereiste persoonsgegevens voor een transactie of dienst 5. de gevolgen van weigering om persoonsgegevens te verstrekken(bijvoorbeeld transacties kunnen niet worden verwerkt) 6. de gevolgen van het weigeren of intrekken van toestemming (bijvoorbeeld uitschrijven voor het ontvangen van informatie over producten en diensten kunnen leiden tot het niet geïnformeerd zijn over verkooppromoties).	Helemaal
CFR02: Als de verwerking is gebaseerd op toestemming van de persoon, moet de entiteit: 1. tijdig de instemming van een persoon verkrijgen en documenteren (dat wil zeggen, op of vóór het tijdstip waarop persoonsgegevens worden verzameld of snel daarna) 2. de voorkeuren van de persoon bevestigen (schriftelijk of elektronisch) 3. de veranderingen in de voorkeuren van een persoon managen en documenteren 4. ervoor zorgen dat de voorkeuren van een persoon tijdig worden doorgevoerd 5. informatie bijhouden om de verkregen toestemming te kunnen aantonen	Grotendeels
CFR03: De entiteit verzamelt of verwerkt geen speciale categorieën van persoonsgegevens, tenzij deze een wettelijke basis heeft om dat te doen. Als de uitdrukkelijke toestemming van de betrokkene de wettige basis vormt voor verwerking van speciale categorieën van persoonsgegevens heeft de betrokkene daarmee uitdrukkelijk toegestemd door middel van enige actie voor het gebruik of openbaren van de speciale categorieën van persoonsgegevens.De entiteit verkrijgt de uitdrukkelijke toestemming rechtstreeks van de betrokkene en bewaart / bewaart bewijs van de gegeven toestemming, bijvoorbeeld door van de persoon te eisen dat hij een vakje aanvinkt of een formulier ondertekend.	Grotendeels
CFR04: In geval de persoonsgegevens worden verwerkt op basis van toestemming van betrokkene zal de entiteit de betrokkene op elk gewenst moment faciliteren bij het uitoefenen van zijn recht om de toestemming in te trekken.	Grotendeels

Toelichting bij deze beheersdoelstelling:
Is geregeld

GDPR Elementen	Privacybeginselen art 5 Rechtmatigheid van verwerking art 6 Voorwaarden voor toestemming, art 7 Rechten van de betrokkene, art 12-19

Verzamelen

Dit privacy-onderwerp betreft de volgende beheersdoelstelling:

- Data Minimalisatie (DMI)

Een beheersdoelstelling kan worden geoperationaliseerd door een of meerdere maatregelen. In het assessment is gevraagd aan te geven in welke mate in de betreffende beheersmaatregelen is voorzien. Daarbij zijn de volgende antwoorden verkregen.

Data Minimalisatie (DMI)

Persoonsgegevens zijn adequaat, relevant en beperkt tot wat nodig is in relatie met de legitieme doeleinden waarvoor de gegevens worden verwerkt.

Beheersmaatregel	**Antwoord**
DMI01: Er zijn een processen en procedures ingesteld om: 1. vast te stellen in hoeverre persoonsgegevens essentieel zijn voor de doeleinden van de verwerking door de entiteit en deze te onderscheiden van optionele persoonsgegevens 2. de verwerking van persoonsgegevens tot het minimum te beperken dat vereist is voor de verwerkingsdoeleinden 3. periodiek de blijvende noodzaak van persoonsgegevens in de producten en/of diensten van de entiteit te beoordelen.	Helemaal
DMI02: In het privacybeleid is dateminimalisatie aangemerkt als een privacyprincipe voor de entiteit (zie Privacybeleid).	Deels

Toelichting bij deze beheersdoelstelling:
Data minimalisatie is voor de eindgebruikers nog steeds een erg lastig onderwerp en leidt tot veel discussie op werkvloer

GDPR Elementen	Privacybeginselen art 5 Privacybeginselen art 5 Privacy by Design/ by Default, art 25

Gebruik, bewaren en verwijderen

Dit privacy-onderwerp betreft de volgende beheersdoelstellingen:

- Gebruiksbeperking (ULI)
- Privacyarchitectuur (Privacy by Design en Privacy by Default) (PBD)
- Dataretentie (DRE)
- Verwijdering, vernietiging en anonimisering (DDA)
- Gebruik en beperking (URE)

Een beheersdoelstelling kan worden geoperationaliseerd door een of meerdere maatregelen. In het assessment is gevraagd aan te geven in welke mate in de betreffende beheersmaatregelen is voorzien. Daarbij zijn de volgende antwoorden verkregen.

Gebruiksbeperking (ULI)

Persoonsgegevens worden niet vrijgegeven, beschikbaar gesteld of anderszins gebruikt voor andere doeleinden dan opgenomen in de privacyverklaring van de entiteit, behalve:
a) met instemming van de betrokkene; of
b) door de autoriteit van de wet.

Beheersmaatregel	Antwoord
ULI01: Een proces en procedures zijn ingesteld om: 1. het openbaren en gebruik van persoonsgegevens te beperken tot de legitieme doeleinden zoals vastgelegd in het privacy beleid van de entiteit en de privacy verklaring 2. continu te verzekeren dat het openbaren en het gebruik van persoonsgegevens in overeenkomst is met de toestemming van de betrokkene en toepasselijke wetgeving en voorschriften.	Helemaal
ULI02: In het privacy beleid is het beperken van gegevensgebruik aangemerkt als een privacy principe voor de entiteit (zie Privacybeleid).	Grotendeels

Toelichting bij deze beheersdoelstelling:
Er is geen gebruik gemaakt van de mogelijkheid om een toelichting te geven bij deze beheersdoelstelling.

GDPR Elementen	Privacybeginselen art 5 Privacybeginselen art 5 Privacy by Design/ by Default, art 25

Privacyarchitectuur (Privacy by Design en Privacy by Default) (PBD)

Bij het ontwerpen of wijzigen van producten, services, bedrijfssystemen of processen houdt de entiteit rekening met een solide privacybeleid, principes en / of toepasselijke wet- en regelgeving.

Beheersmaatregel	Antwoord

PBD01: Bij het ontwikkelen, ontwerpen, selecteren en gebruiken van toepassingen, services en producten welke persoonsgegevens verwerken, houdt de entiteit zo vroeg mogelijk in de ontwerp fase rekening met de privacy beginselen en privacy risico's. Het risico van conflicten tussen het privacy ontwerp en de rechten en vrijheden van betrokkenen (en het privacy beleid van de entiteit) worden geïdentificeerd en geadresseerd. Als derden bij deze activiteiten zijn betrokken, vereist de entiteit van deze derden om dezelfde activiteiten voor risicobeheersing uit te voeren.	Deels
PBD02: Beoordeling van privacy risico's is een inherent en gedocumenteerd onderdeel van de projectmethodologie en/of ontwerp en ontwikkeling werkwijze van de entiteit.	Deels
PBD03: Als systemen, services en producten persoonsgegevens verwerken en privacy-gerelateerde keuzes en opties bieden, dan zijn de standaardinstellingen zo restrictief mogelijk ingesteld, dit met het oogpunt op privacy.	Deels

Toelichting bij deze beheersdoelstelling:
Met name bij leverancier van de ERP/software liggen nog aandachtspunten

GDPR Elementen	Privacybeginselen art 5 Privacybeginselen art 5 Privacy by Design/ by Default, art 25

Dataretentie (DRE)

Persoonsgegevens worden niet langer bewaard dan de minimale tijd:
- zoals vereist door toepasselijke wet- en regelgeving;
- die nodig is voor de doeleinden waarvoor de gegevens zijn verzameld.

Beheersmaatregel	**Antwoord**
DRE01: De entiteit: 1. documenteert haar bewaarbeleid en verwijderingsprocedures voor persoonsgegevens 2. waarborgt dat persoonsgegevens niet worden bewaard buiten de gevestigde retentietijd tenzij daarvoor een gerechtvaardigde zakelijke of wettelijke reden voor bestaat 3. voor elke verwerking van persoonsgegevens liggen de retentietijden vast 4. openbaart het bewaartermijnbeleid aan betrokkenen in haar privacy verklaring 5. bewaart, slaat op, verwijdert gearchiveerde back-upkopieën van gegevens records, conform haar bewaarbeleid.	Helemaal
DRE02: Als het verwijderen, vernietigen of het beperken van gegevens leidt tot uitzonderingen op het normale beleid, worden contractuele vereisten (her) overwogen.	Deels

Toelichting bij deze beheersdoelstelling:
Er is geen gebruik gemaakt van de mogelijkheid om een toelichting te geven bij deze beheersdoelstelling.

GDPR Elementen	Privacybeginselen art 5 Privacybeginselen art 5 Verantwoordelijkheden van verantwoordelijke en verwerker, art 24,28

Verwijdering, vernietiging en anonimisering (DDA)

Persoonsgegevens worden waar nodig geanonimiseerd en/of verwijderd binnen de entiteit. Identiteiten mogen niet identificeerbaar zijn en persoonsgegevens mogen niet meer beschikbaar zijn na de bewaartermijn.

Beheersmaatregel	Antwoord
DDA01: De entiteit heeft een gedocumenteerd proces dat ervoor zorgt dat: 1. het wissen of vernietigen van persoonsgegevensrecords in overeenstemming is met het bewaarbeleid, ongeacht de aard van de opslag media (bijvoorbeeld elektronische, optische media of papier) 2. de verwijdering van origineel, gearchiveerd, back-up en ad hoc of persoonlijke kopieën van bestanden in overeenstemming is met het vernietigingsbeleid 3. adequate documentatie over de verwijdering van persoonsgegevens beschikbaar is 4. openbaart het bewaartermijnbeleid aan betrokkenen in haar privacy verklaring 5. bewaart, slaat op, verwijdert gearchiveerde back-upkopieën van gegevens records, conform haar bewaarbeleid. De entiteit zorgt er verder voor dat: • - binnen de grenzen van de technologie, gegevens over een persoon lokaliseert, verwijdert of vermindert , bijvoorbeeld verwijderen creditcardnummers nadat de transactie is voltooid • - regelmatig en systematisch persoonsgegevens vernietigt, wist of anonimiseert als deze niet langer nodig zijn om de geïdentificeerde doelen of zoals te vervullen vereist door weten regelgeving.	Grotendeels
DDA02: Als de verwijdering vernietiging en reductiepraktijken kunnen leiden tot een uitzondering op het normale beleid van de entiteit worden contractuele vereisten in (her)overweging genomen.	Grotendeels

Toelichting bij deze beheersdoelstelling:
Het verwijderen na afloop van de bewaartijd gebeurt niet goed en consequent

GDPR Elementen	Privacybeginselen art 5 Privacybeginselen art 5 Privacy by Design/ by Default, art 25 Verantwoordelijkheden van verantwoordelijke en verwerker, art 24,28 Beveiliging van de verwerking, art 32

Gebruik en beperking (URE)

Persoonsgegevens worden niet gebruikt in geval van beperking door de betrokkene of in geval van specifieke wettelijke beperkingen door de lokale overheid. Bezwaren tegen de verwerking door de betrokkene zullen adequaat worden behandeld.

Beheersmaatregel	Antwoord
URE01: De entiteit communiceert met de betrokkene de stappen om gebruik te kunnen maken van het recht op beperking van de verwerking, het recht om bezwaar aan te tekenen tegen de verwerking en de criteria om dit te doen.	Helemaal
URE02: De entiteit heeft een proces om adequaat te reageren op betrokkenen om hun rechten uit te oefenen op de beperking van verwerking of bezwaar aan tekenen tegen het verwerken.	Helemaal

URE03: De entiteit heeft vastgesteld of de lokale wetgeving van de lidstaat beperkingen oplegt op de verwerking van persoonsgegevens (bijvoorbeeld ter bescherming van nationale of openbare veiligheid) en voldoet aantoonbaar aan deze beperkingen.	Helemaal

Toelichting bij deze beheersdoelstelling:
Er is geen gebruik gemaakt van de mogelijkheid om een toelichting te geven bij deze beheersdoelstelling.

GDPR Elementen	Privacybeginselen art 5 Privacybeginselen art 5 Rechtmatigheid van verwerking art 6 Rechten van de betrokkene, art 12-19 Overdracht van persoonsgegevens aan derde landen of internationale organisaties, art 44-50

Datatoegang en datakwaliteit

Dit privacy-onderwerp betreft de volgende beheersdoelstellingen:

- Data toegangsverzoeken (DAR)
- Data correctie verzoeken (DCR)
- Data verwijdering verzoeken (DDR)
- Data overdracht verzoeken (DPR)
- Nauwkeurigheid en volledigheid van gegevens (ACD)

Een beheersdoelstelling kan worden geoperationaliseerd door een of meerdere maatregelen. In het assessment is gevraagd aan te geven in welke mate in de betreffende beheersmaatregelen is voorzien. Daarbij zijn de volgende antwoorden verkregen.

Data toegangsverzoeken (DAR)

Een verzoek om toegang van betrokkene wordt adequaat beantwoord en betrokkene wordt in staat gesteld vast te stellen welke persoonsgegevens over hem/haar worden verwerkt en op welke manier.

Beheersmaatregel	Antwoord
DAR01: Er zijn procedures om adequaat te reageren op verzoeken om toegang van betrokkene. Indien de betrokkene zijn / haar recht uitoefent, zal de entiteit de betrokkene informeren over de aard van de verwerkte persoonsgegevens en de kenmerken van de verwerking (bijvoorbeeld doel, ontvangers, retentietijden, het bestaan van geautomatiseerde besluitvorming).	Grotendeels
DAR02: De entiteit informeert de betrokkene over het bestaan van dit recht en de procedure om van dit recht gebruik te maken in de privacyverklaring.	Helemaal
DAR03: De entiteit heeft een procedure geïmplementeerd om de betrokkene in een gangbare elektronische vorm tijdig een kopie te geven van de verwerkte persoonsgegevens.	Helemaal
DAR04: De entiteit verifieert de identiteit van de betrokken voordat wordt gereageerd op het verzoek.	Helemaal

Toelichting bij deze beheersdoelstelling:
Is ingebed bij P&O

GDPR Elementen	Privacybeginselen art 5 Rechten van de betrokkene, art 12-19 Privacy by Design/ by Default, art 25 Beveiliging van de verwerking, art 32

Data correctieverzoeken (DCR)

Verzoeken om correcties van gegevens worden adequaat beantwoord en betrokkenen worden in staat gesteld na te gaan of hun persoonsgegevens juist / up-to-date zijn hun persoonsgegevens te laten corrigeren.

Beheersmaatregel	Antwoord

DCR01: Er is voorzien in procedures om adequaat te reageren op verzoeken tot correctie. Als de betrokkene van dit recht gebruik maakt, zal de entiteit de persoonsgegevens van de betrokkene zonder onnodige vertraging corrigeren.	Helemaal
DCR02: De entiteit informeert de betrokkene over het bestaan van dit recht en de procedure om dit uit te oefenen in de privacyverklaring.	Helemaal
DCR03: De entiteit verifieert de identiteit van de betrokkene voordat het verzoek wordt uitgevoerd.	Helemaal
DCR04: De entiteit stelt derden, aan wie persoonsgegevens zijn bekend gemaakt, op de hoogte over noodzakelijke correcties in persoonsgegevens.	Grotendeels

Toelichting bij deze beheersdoelstelling:
Er is geen gebruik gemaakt van de mogelijkheid om een toelichting te geven bij deze beheersdoelstelling.

GDPR Elementen	Privacybeginselen art 5 Rechten van de betrokkene, art 12-19

Data verwijderingsverzoeken (DDR)

Verzoeken om verwijdering van gegevens worden adequaat beantwoord en betrokkenen kunnen hun persoonsgegevens laten verwijderen als aan relevante criteria wordt voldaan.

Beheersmaatregel	**Antwoord**
DDR01: Er is voorzien in procedures om adequaat te reageren op verzoeken tot verwijderen van gegevens (recht om te worden vergeten). Als de betrokkene zijn/haar recht uitoefent, zal de entiteit de gronden van het verzoek toetsen aan de toepasselijke criteria (bijvoorbeeld verwerking is gebaseerd op toestemming, onwettige verwerking, doel niet langer geldig, wettelijke vereisten voor retentie). Als een geldige reden bestaat, zal de entiteit de persoonsgegevens zonder onnodige vertraging wissen.	Helemaal
DDR02: Indien van toepassing, informeert de entiteit andere verantwoordelijken, aan wie de persoonsgegevens zijn doorgegeven, over het verzoek van de betrokkene om persoonsgegevens verwijderden.	Helemaal
DDR03: De entiteit informeert de betrokkene over het bestaan van dit recht en de procedure om dit recht uit te oefenen in de privacyverklaring.	Helemaal
DDR04: De entiteit verifieert eerst de identiteit van de betrokkenen voordat het verzoek wordt uitgevoerd.	Helemaal

Toelichting bij deze beheersdoelstelling:
P&O wikkelt dit goed af volgens vastgestelde procedures

GDPR Elementen	Privacybeginselen art 5 Rechten van de betrokkene, art 12-19

Data overdrachtverzoeken (DPR)

Verzoeken om gegevens over te dragen worden adequaat beantwoord en betrokkenen kunnen hun persoonsgegevens aan een andere entiteit laten overdragen indien aan de toepasselijke criteria is voldaan.

Beheersmaatregel	Antwoord
DPR01: Er is voorzien in procedures om adequaat te reageren op de verzoeken voor het overdragen van gegevens. Als de betrokkene zijn/haar recht uitoefent, zal de entiteit de redenen van het verzoek toetsen aan de hand van toepasselijke criteria (bijvoorbeeld verwerking is gebaseerd op toestemming, de verwerking gebeurt geautomatiseerd). Als een geldige reden bestaat, draagt de entiteit de persoonlijke gegevens over, zonder onnodige vertraging.	Helemaal
DPR02: Indien technisch mogelijk, zal de entiteit de persoonsgegevens rechtstreeks aan een andere (controlerende) entiteit overdragen, zoals aan gegeven door de betrokkene.	Helemaal
DPR03: De entiteit informeert de betrokkene over het bestaan van dit recht en de procedure om dit recht uit te oefenen in de privacyverklaring.	Helemaal
DPR04: De entiteit verifieert de identiteit van de betrokkene voordat het verzoek wordt uitgevoerd.	Helemaal

Toelichting bij deze beheersdoelstelling:
P&O wikkelt dit goed af volgens vastgestelde procedures

GDPR Elementen	Privacybeginselen art 5 Rechten van de betrokkene, art 12-19 Recht op gegevensportabiliteit, art 20

Nauwkeurigheid en volledigheid van gegevens (ACD)

Gedocumenteerde procedures voor het valideren, het bewerken en het actualiseren van persoonsgegevens waarborgen een accurate en volledige verwerking van en de toegang tot persoonsgegevens wanneer dat nodig is.

Beheersmaatregel	Antwoord
ACD01: De entiteit heeft voorzien in procedures om: 1. persoonsgegevens te bewerken en valideren bij het verzamelen, aanmaken, onderhouden en bijwerken 2. de datums te registreren waarop de persoonsgegevens zijn verkregen of bijgewerkt 3. te specificeren wanneer de persoonsgegevens niet meer geldig zijn 4. te specificeren wanneer en hoe de persoonsgegevens moeten worden bijgewerkt en de bron van de update (bijvoorbeeld jaarlijkse herbevestiging van informatie en methoden voor individuen om proactief de persoonsgegevens bij te werken) 5. aan te geven hoe de juistheid en volledigheid van persoonsgegevens wordt gecontroleerd van gegevens welke rechtstreeks worden ontvangen van een derde partij, of bekend gemaakt aan een derde partij 6. ervoor zorgen dat de verwerkte persoonsgegevens voldoende nauwkeurig en compleet zijn om beslissingen te nemen.	Deels
ACD02: De entiteit voert periodieke beoordelingen uit op de nauwkeurigheid van persoonsgegevens en waar nodig te corrigeren om te kunnen voldoen aan het gestelde doel.	Grotendeels

Toelichting bij deze beheersdoelstelling:
Er is geen gebruik gemaakt van de mogelijkheid om een toelichting te geven bij deze beheersdoelstelling.

GDPR Elementen	Privacybeginselen art 5 Beveiliging van de verwerking, art 32

Openbaar maken

Dit privacy-onderwerp betreft de volgende beheersdoelstellingen:

- Openbaarmaking en registratie door derden (TPD)
- Derdenovereenkomsten (TPA)
- Gegevensoverdracht (DTR)

Een beheersdoelstelling kan worden geoperationaliseerd door een of meerdere maatregelen. In het assessment is gevraagd aan te geven in welke mate in de betreffende beheersmaatregelen is voorzien. Daarbij zijn de volgende antwoorden verkregen.

Openbaarmaking en registratie door derden (TPD)

Persoonsgegevens worden niet bekendgemaakt aan derden of verder verwerkt voor doeleinden waarvoor het individu niet heeft toegestemd.

Beheersmaatregel	Antwoord
TPD01: De entiteit heeft voorzien in procedures om: 1. te voorkomen dat persoonsgegevens aan derden worden bekendgemaakt, tenzij de betrokkene hiervoor toestemming heeft gegeven 2. de aard en omvang van de persoonsgegevens welke worden ontsloten aan derden te documenteren 3. te controleren of de ontsluiting aan derden steeds compliant is met het privacy beleid en de procedures van de entiteit, of specifiek is toegestaan of vereist door wet- of regelgeving 4. het openbaar maken aan/van derde partijen om juridische redenen te documenteren 5. individuen te infomeren en hun toestemming te krijgen voorafgaand aan het openbaren van persoonsgegevens aan een derde partij, voor doeleinden welke niet zijn opgenomen in de privacy verklaring 6. te bewaken dat persoonsgegevens alleen aan derden worden verstrekt als de doeleinden zijn opgenomen in de privacyverklaring.	Grotendeels

Toelichting bij deze beheersdoelstelling:
Vanuit overheid komen veel verzoeken en dit is niet altijd vooraf afgestemd

GDPR Elementen	Privacybeginselen art 5 Rechtmatigheid van verwerking art 6 Beveiliging van de verwerking, art 32

Derdenovereenkomsten (TPA)

Privacyoverwegingen en -vereisten worden adequaat behandeld bij de aanschaf van (op persoonsgegevens betrekking hebbende) oplossingen of diensten van derden, resulterend in een gepaste verwerking of bescherming van persoonsgegevens.

Beheersmaatregel	Antwoord

TPA01: Als de entiteit oplossingen verwerft van derden/leveranciers of processen uit besteedt aan serviceproviders en de verwerking van persoonsgegevens wordt (gedeeltelijk) gecontracteerd, sluit de entiteit formele overeenkomsten waarin met de derde partij wordt overeengekomen dat deze de zorgvuldigheid een niveau van bescherming van persoonsgegevens hanteert dat gelijkwaardig is aan het niveau van de entiteit. Door dit te doen beperkt de entiteit het gebruik door derden van persoonsgegevens tot de doeleinden van de entiteit.	Helemaal
TPA02: De entiteit zorgt ervoor dat overeenkomsten met derden ook verplichtingen van de derde partij omvatten met betrekking tot: 1. vertrouwelijkheid en niet-openbaarmaking 2. beveiligingsvereisten 3. samenwerking bij het reageren op verzoeken van betrokkenen en de uitvoering daarvan 4. informatievoorziening (bijvoorbeeld in het geval van geplande onder aanneming) 5. informatieverschaffing en samenwerking in het geval van datalekken 6. bewaartermijnen en verwijdering van gegevens 7. geen verdere uitbesteding zonder toestemming van de entiteit 8. aansprakelijkheden en vrijwaringen	Grotendeels
TPA03: De entiteit evalueert de prestaties en compliance van derden met behulp van een of meer van de volgende benaderingen (in oplopende volgorde van zekerheid en afhankelijk van het risicoprofiel van de derde): 1. de derde partij reageert op een vragenlijst over haar praktijken 2. de derde partij verklaart zelf dat zijn praktijken voldoen aan de vereisten van de entiteit op basis van interne auditrapporten of andere procedures 3. de entiteit voert een periodieke evaluatie ter plaatse van de derde uit 4. de entiteit verkrijgt een audit- of assurance beoordeling door een onafhankelijke auditor.	Grotendeels

Toelichting bij deze beheersdoelstelling:
Er is geen gebruik gemaakt van de mogelijkheid om een toelichting te geven bij deze beheersdoelstelling.

GDPR Elementen	Privacybeginselen art 5 Verantwoordelijkheden van verantwoordelijke en verwerker, art 24,28 Beveiliging van de verwerking, art 32

Gegevensoverdracht (DTR)

Persoonsgegevens worden niet overgedragen naar landen met een ontoereikend wettelijk privacyregime (dat wil zeggen verplaatsing, weergave of afdrukken van gegevens op een andere locatie).

Deze beheersdoelstelling is door de invuller buiten scope gesteld. Derhalve zijn de bijbehorende vragen hier niet gerapporteerd.

GDPR Elementen	Privacybeginselen art 5 Overdracht van persoonsgegevens aan derde landen of internationale organisaties, art 44-50

Data beveiliging

Dit privacy-onderwerp betreft de volgende beheersdoelstellingen:

- Informatiebeveiligingsprogramma (ISP)
- Identiteits- en toegangsbeheer (IAM)
- Veilige verzending (STR)
- Encryptie en eindpuntbeveiliging (ENC)

Een beheersdoelstelling kan worden geoperationaliseerd door een of meerdere maatregelen. In het assessment is gevraagd aan te geven in welke mate in de betreffende beheersmaatregelen is voorzien. Daarbij zijn de volgende antwoorden verkregen.

Informatiebeveiligingsprogramma (ISP)

Persoonsgegevens zijn adequaat beveiligd tegen onopzettelijke fouten, verlies, tegen kwaadwillende handelingen zoals hacking, opzettelijke diefstal, openbaarmaking of verlies.

Beheersmaatregel	Antwoord
ISP01: De entiteit heeft passende technische en organisatorische maatregelen getroffen om de beveiliging van persoonsgegevens te waarborgen. Beveiliging omvat vertrouwelijkheid, integriteit en beschikbaarheid van persoonsgegevens. (Zie ook identiteits- en toegangsbeheer, veilige verzending, encryptie en eindpuntbeveiliging en logging van toegang.)	Grotendeels
ISP02: Beveiliging van persoonsgegevens wordt expliciet behandeld in het informatiebeveiligingsbeleid en het beheer van informatiebeveiligingssysteem van de entiteit.	Grotendeels
ISP03: De geschiktheid van beveiligingsmaatregelen met betrekking tot persoonsgegevens is vastgesteld in periodieke risicobeoordelingen waarin alle relevante stakeholders deelnemen en waarin de actuele en de geplande verwerking van persoonsgegevens wordt beoordeeld.	Grotendeels
ISP04: De entiteit heeft een gedocumenteerd beleid inzake versleuteling en pseudonimisering van persoonsgegevens en controleert systematisch de naleving van het beleid (zie ook bij encryptie STR en ENC).	Niet
ISP05: De entiteit test, evalueert en evalueert regelmatig de effectiviteit van technische en organisatorische beveiligingsmaatregelen om te zorgen voor een adequate niveau van beveiliging van persoonsgegevens en om verbeteringen te identificeren en te initiëren.	Deels
ISP06: De entiteit heeft een actieve houding ten opzichte van het inzetten van een gedragscode (van verenigingen of brancheorganisaties) en/of certificeringen) om een passend niveau van beveiliging van persoonsgegevens aan te tonen.	Grotendeels
ISP07: Het beveiligingsplan van de entiteit voorkomt toegang tot persoonsgegevens in computers, media en op papier gebaseerde informatie welke niet langer in de computer zit en niet langer actief wordt gebruikt. Bijvoorbeeld computers, media en papieren informatie in opslag,welke zijn verkocht of anderszins verwijderd).	Grotendeels

Toelichting bij deze beheersdoelstelling:
Er is wel beleid maar naleving en controle laat te wensen over en kan veel beter

GDPR Elementen	Privacybeginselen art 5 Beveiliging van de verwerking, art 32

Identiteits- en toegangsbeheer (IAM)

Toewijzing van passende toegangsrechten, passende wijzigingen in toegangsrechten en tijdige verwijdering van toegangsrechten verminderen de kans op ongeoorloofde toegang tot of ongepaste behandeling van persoonlijke gegevens, of datalekken door interne medewerkers, derde partijen of hackers.

Beheersmaatregel	Antwoord
IAM01: Er is voorzien in systemen en procedures om: 1. het niveau en de aard van de toegang voor de gebruikersrechten vast te stellen, rekenend houdende met de gevoeligheid van de persoonsgegevens en de legitieme zakelijke behoefte van de gebruiker voor toegang tot de persoonsgegevens 2. gebruikers te authentiseren, bijvoorbeeld op gebruikersnaam en wachtwoord, certificaat, externe token of biometrische gegevens voordat toegang wordt verleend tot systemen welke persoonsgegevens verwerken 3. sterkere beveiligingsmaatregelen te vereisen voor externe toegang, zoals extra of dynamische wachtwoorden, terugbelprocedures, digitale certificaten, beveiligde IDkaarten, virtueel particulier netwerk (VPN), of deugdelijk geconfigureerde firewalls 4. intrusion detection en monitoring systemen te implementeren.	Deels

Toelichting bij deze beheersdoelstelling:
Er is wel bveiliging maar deze is voor de zwaardere rollen niet afdoende (bijvoorbeeld dubbele identificatie vanuit verschillende bronnen)

GDPR Elementen	Privacybeginselen art 5 Beveiliging van de verwerking, art 32

Veilige verzending (STR)

Beperkte toegang tot persoonsgegevens tijdens de verzending verhindert op gepaste wijze onbevoegde openbaarmaking, schending, wijziging of vernietiging van persoonsgegevens.

Beheersmaatregel	Antwoord
STR01: Er is voorzien in systemen en procedures om: 1. minimale niveaus van encryptie en controles te definiëren 2. industriestandaard coderingstechnologie voor overdracht en ontvangst van persoonsgegevens te gebruiken 3. externe netwerkverbindingen te beoordelen en goed te keuren 4. persoonsgegevens te beschermen zowel bij papieren als elektronische formulieren per post, koerier of andere fysieke middelen 5. persoonsgegevens te versleutelen welke draadloos worden verzameld en verzonden en het beveiligen van draadloze netwerken tegen ongeoorloofde toegang.	Grotendeels

Toelichting bij deze beheersdoelstelling:
Veilig mailen is aangeschaft

GDPR Elementen	Privacybeginselen art 5 Beveiliging van de verwerking, art 32 Persoonlijke gegevens inbreuk, art 33, 34

Encryptie en end-point security (ENC)

Versleuteling verzekerd de preventie van een inbreuk op persoonsgegevens (onopzettelijk verlies van persoonsgegevens of kwaadwillende handelingen zoals opzettelijke diefstal, openbaarmaking of verlies).

Beheersmaatregel	Antwoord
ENC01: Beleid en procedures verbieden de opslag van persoonsgegevens gegevens op draagbare apparaten media of apparaten tenzij een zakelijke behoefte bestaat en dergelijke opslag is goedgekeurd door het management.	
ENC02: Er is voorzien in beleid, systemen en procedures om de toegang tot persoonsgegevens te beschermen welke zijn opgeslagen op apparaten zoals: 1. laptops, PDA's, smartphones en soortgelijke apparaten 2. computers en andere apparaten welke door werknemers worden gebruikt bijvoorbeeld voor werken onderweg/thuis 3. USB-drives, CD's en DVD's, magnetische tape of andere draagbare media Dergelijke informatie is versleuteld, beveiligd met een wachtwoord, fysiek beschermd en onderwerp van het beleid van de entiteit inzake toegang, retentie en vernietiging van persoonsgegevens.	
ENC03: Er is voorzien in procedures voor het maken, overdragen, opslaan en verwijderen van media welke worden gebruikt voor back-up en herstel van persoonsgegevens.	
ENC04: Er is voorzien in procedures om verlies of potentieel misbruik van media welke persoonsgegevens bevatten te rapporteren (zie ook PIA).Bij beëindiging van een dienstverband - of contracten van derden zijn er procedures om te voorzien in het inleveren of vernietiging van draagbare media en apparaten welke worden gebruikt voor toegang en opslag van persoonsgegevens en van gedrukte en andere kopieën van dergelijke informatie.	

Toelichting bij deze beheersdoelstelling:
Er is geen gebruik gemaakt van de mogelijkheid om een toelichting te geven bij deze beheersdoelstelling.

GDPR Elementen	Privacybeginselen art 5 Beveiliging van de verwerking, art 32 Persoonlijke gegevens inbreuk, art 33, 34

Logging van toegang (LOG)

De entiteit detecteert en onderzoekt toegangs- of toegangspogingen tot persoonsgegevens door personeel, derden of hackers die kunnen leiden tot een inbreuk, sabotage van systemen, invoeging van kwaadwillige code, diefstal van persoonsgegevens, etc.

Beheersmaatregel	Antwoord

LOG01: Er is voorzien in systemen en procedures voor: 1. het beheer van logische en fysieke toegang tot persoons gegevens, inclusief papieren exemplaren, archief- en reservekopieën 2. het loggen en controleren van de toegang (pogingen) tot systemen met persoonsgegevens in een logbestand met een detailniveau en retentietijd welke voldoende is voor de doeleinden van analyse en onderzoek 3. te voorkomen dat ongeoorloofd of per ongeluk persoonsgegevens worden vernietigt of verloren gaan 4. het onderzoeken van schendingen en pogingen om ongeautoriseerde toegang te krijgen.	Helemaal

Toelichting bij deze beheersdoelstelling:
Er is geen gebruik gemaakt van de mogelijkheid om een toelichting te geven bij deze beheersdoelstelling.

GDPR Elementen	Privacybeginselen art 5 Beveiliging van de verwerking, art 32 Persoonlijke gegevens inbreuk, art 33, 34

Monitoring en handhaving

Dit privacy-onderwerp betreft de volgende beheersdoelstellingen:

- Herziening van privacy-compliance (REV)
- Periodieke monitoring van privacy-controles (MON)

Een beheersdoelstelling kan worden geoperationaliseerd door een of meerdere maatregelen. In het assessment is gevraagd aan te geven in welke mate in de betreffende beheersmaatregelen is voorzien. Daarbij zijn de volgende antwoorden verkregen.

Herziening van privacy-compliance (REV)

Adequaat toezicht op de interne organisatie en derden zorgen voor naleving van toepasselijke privacywetten en wettelijke vereisten en vermindert het risico van datalekken of verlies van persoonsgegevensgegevens.

Beheersmaatregel	Antwoord
REV01: Er is voorzien in systemen en procedures om: 1. jaarlijks de naleving te toetsen van privacy beleid en -procedures, verplichtingen en toepasselijke wetten, voorschriften, serviceniveau overeenkomsten, door de entiteit aangenomen standaarden/normen en andere contracten 2. periodieke beoordelingen vast te leggen, bijvoorbeeld interne auditplannen, auditrapporten, compliance controlelijsten en vaststelling door het management 3. resultaten te rapporteren van de compliance review en aanbevelingen voor verbetering van het beheer en een herstelplan uit te voeren 4. toezicht te houden op de oplossing van problemen en kwetsbaarheden uit de compliance review om ervoor te zorgen dat tijdig passende corrigerende maatregelen worden genomen (inclusief herziening van het privacy beleid en procedures, indien nodig).	Deels

Toelichting bij deze beheersdoelstelling:
Er is geen gebruik gemaakt van de mogelijkheid om een toelichting te geven bij deze beheersdoelstelling.

GDPR Elementen	Privacybeginselen art 5 Rechtmatigheid van verwerking art 6

Periodieke monitoring van privacy-controles (MON)

De entiteit beoordeelt systematisch en periodiek privacyprocessen en -controles om vast te stellen dat deze werken zoals ontworpen, resulterend in voortdurende naleving van toepasselijke wetten, regels en vereisten.

Beheersmaatregel	Antwoord

MON01: Om de effectiviteit van de privacy beheersmaatregelen van de entiteit te waarborgen beoordeelt het management: 1. beheersingsoutput, controlerapporten en afwijkingen 2. trendanalyse 3. training aanwezigheid en evaluaties van trainingen 4. klachten en oplossingen 5. interne beoordelingen 6. interne en externe auditrapporten 7. onafhankelijke audit / assurance-rapporten over privacy controle's bij serviceorganisaties 8. ander bewijs van de effectiviteit van beheersmaatregelen	
MON02: De selectie van te bewaken, te controleren en/of te controleren beheersmaatregelen en de frequentie waarmee de monitoring wordt uitgevoerd, is gebaseerd op de gevoeligheid van de betrokken persoonsgegevens en de risico's van mogelijke blootstelling of verlies.	Deels
MON03: De entiteit voorziet in een proces dat zorgt voor monitoring, herstel van tekortkomingen en voortdurende verbetering.	Deels

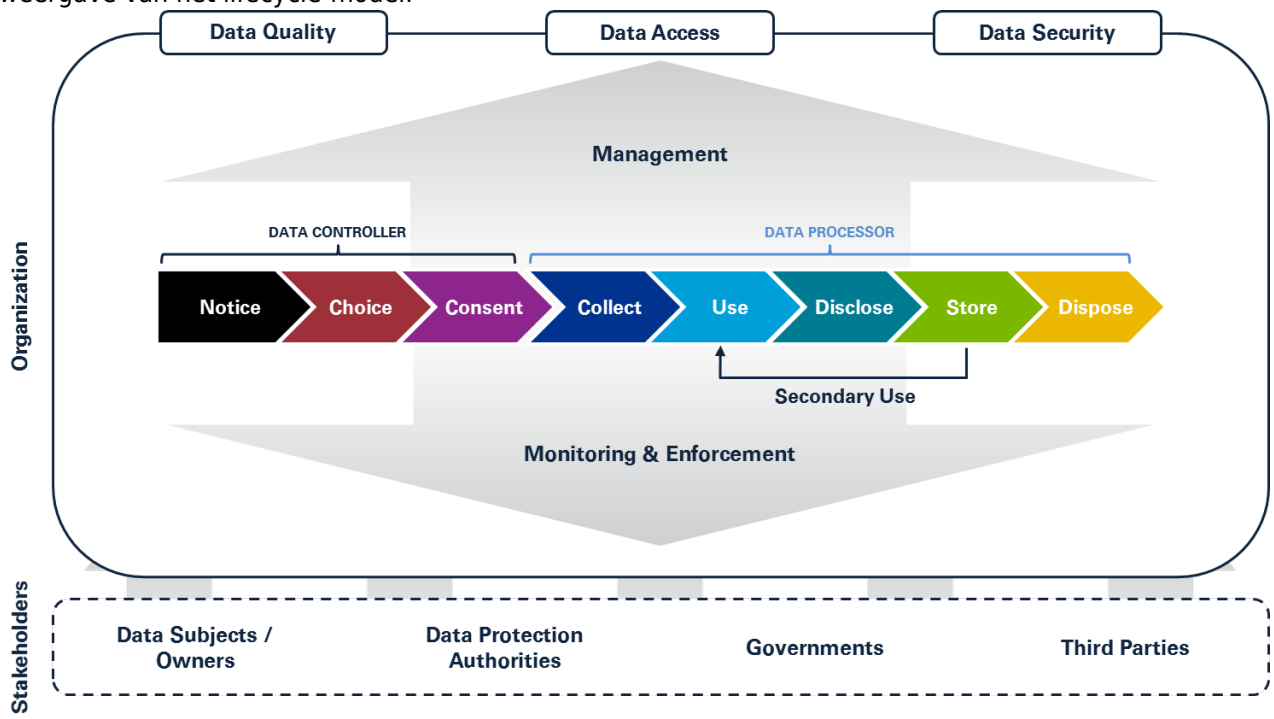
Toelichting bij deze beheersdoelstelling:
Niet jaarlijks, meer als er iets nieuws voorbijkomt, dus niet periodiek ingebed

GDPR Elementen	Privacybeginselen art 5 Rechtmatigheid van verwerking art 6

Bijlage I Informatie Lifecycle Management

Introductie

Het PCF is gestructureerd volgens een Information Lifecycle-model. Onderstaand een grafische weergave van het lifecycle-model:



Voor meer informatie: Publicatie in de IT Auditor

Verschillende fasen

Het informatie levenscyclusmodel is gebaseerd en gedefinieerd op basis van een mix van GAPP-principes en OECD-principes. Het Information Lifecycle-model bestaat uit 8 verschillende fasen:

1. **Kennisgeven:** de levenscyclus van informatie begint met het informeren van de betrokkene over het gebruik van zijn persoonlijke gegevens. De entiteit verstrekt kennisgeving over haar privacybeleid en -procedures en identificeert de doeleinden waarvoor persoonlijke informatie wordt verzameld, gebruikt, bewaard en openbaar gemaakt.

2. **Keuze:** de entiteit beschrijft de verschillende keuzes die de betrokkene ter beschikking staan met betrekking tot het verzamelen, het gebruik en de openbaarmaking van persoonlijke informatie door de entiteit.

3. **Toestemmen:** de entiteit stelt de impliciete of expliciete instemming veilig van de betrokkene met betrekking tot het verzamelen, het gebruik en de bekendmaking van de persoonsgegevens.

4. **Verzamelen:** Persoonlijke informatie wordt alleen door de entiteit verzameld voor de doeleinden die in de fase Kennisgeven zijn geïdentificeerd.

5. **Gebruiken:** De entiteit beperkt het gebruik van persoonlijke informatie tot de doeleinden die in de fase Kennisgeven zijn geïdentificeerd en waarvoor de betrokkene impliciet of expliciet toestemming heeft gegeven.

6. **Openbaar maken:** de entiteit onthult persoonlijke informatie uitsluitend aan derden voor de doeleinden die in de fase Kennisgeven en met de impliciete of expliciete toestemming van de betrokkene zijn benoemd.

7. **Bewaren:** De entiteit bewaart persoonlijke informatie niet langer dan nodig is voor t het doel zoals gedefinieerd in de fase Kennisgeven of zoals vereist door wet- en regelgeving. De mogelijkheid bestaat dat persoonlijke gegevens worden hergebruikt ('secundair gebruik') en terugvloeien naar de fase Gebruik, alleen als de doeleinden voor secundair gebruik overeenkomen met die in de fase Kennisgeven.

8. **Verwijderen:** de entiteit beschikt op gepaste wijze over persoonlijke informatie.

Life cycle Matrix verantwoordelijkheden		
Partij	Fasen	Toelichting
Verantwoordelijke	**1. Kennisgeven** **2. Keuze** **3. Toestemmen**	In deze processen worden persoonsgegevens van betrokkenen (nog) niet verwerkt. De verwerking van persoonsgegevens wordt voorbereid door de verantwoordelijke voor de verwerking van gegevens zodat : aan de vereisten wordt voldaan voordat de verwerking van persoonsgegevens daadwerkelijk kan plaatsvinden.
Verwerker	**4. Verzamelen** **5. Gebruik** **6. Openbaar maken** **7. Bewaren** **8. Verwijderen**	Dit is de entiteit die de persoonsgegevens feitelijk verwerkt (dit kan ook de Verantwoordelijke zijn).

Randvoorwaarden - management en stakeholders

Het management bepaalt de richting (bijvoorbeeld de privacystrategie, het privacybeleid, enz.) en zorgt ervoor dat persoonlijke gegevens op gecontroleerde wijze door de verschillende fasen van de informatie-lifecycle stromen (Monitoring and Handhaving). Over het algemeen zijn er drie voorwaarden voor persoonlijke gegevens in de verschillende fasen van de levenscyclus van informatie om ervoor te zorgen dat bedrijfsprocessen accuraat, volledig en tijdig werken:

- Data kwaliteit;
- Toegang tot data;
- Dataveiligheid.

Ten slotte presenteert het levenscyclusmodel ook de verschillende externe belanghebbenden met betrekking tot de verschillende fasen in de verwerking van persoonsgegevens. Deze belanghebbenden hebben betrekking op:

- Betrokkenen;
- Autoriteiten voor gegevensbescherming (bijv Autoriteit Persoonsgegevens in Nederland);
- Overheden;
- Derden (of gegevensverwerkers).

Op basis van dit conceptuele model is een Privacy Control Framework (PCF) ontwikkeld, dat een overzicht van besturingsdoelstellingen en bijbehorende beheersmaatregelen bevat. De besturingsdoelen zijn gegroepeerd volgens de verschillende fasen die worden genoemd in het lifecycle-informatiemodel.

Op deze manier is een duidelijk overzicht aanwezig van de verschillende doelstellingen voor privacybeheer die zijn gepositioneerd in de fasen van het lifecycle-informatiemodel. We kunnen concluderen dat het gebruik van dit model het beheer van persoonsgegevens in entiteiten aanzienlijk kan worden verbeterd.

Bijlage II Uitkomsten assessment per beheersdoelstelling

Levenscyclus	Onderwerp	#	H	G	D	N	n/a	NI
Beheer	Privacy beleid (PPO)	5	1	4	0	0	0	0
	Definitie van rollen en verantwoordelijkheden (RRE)	5	2	2	1	0	0	0
	Identificatie en classificatie van persoonlijke gegevens (PDI)	4	0	4	0	0	0	0
	Risk Management (RMA)	5	0	1	2	2	0	0
	Gegevensbeschermingseffectrapportages (PIA)	6	0	5	1	0	0	0
	Privacy Incident en Breach Management (PIB)	9	1	6	0	2	0	0
	Personeelsbevoegdheden (SCO)	4	0	1	2	1	0	0
	Bewustwording en training van personeel (SAT)	3	0	0	0	3	0	0
	Juridische beoordeling van wijzigingen in wettelijke en / of zakelijke vereisten (LRC)	1	0	1	0	0	0	0
Kennisgeving	Privacyverklaring (PST)	2	1	1	0	0	0	0
Keuze en toestemming	Toestemmingskader (CFR)	4	1	3	0	0	0	0
Verzamelen	Data Minimalisatie (DMI)	2	1	0	1	0	0	0
Gebruik, bewaar en verwijder	Gebruiksbeperking (ULI)	2	1	1	0	0	0	0
	Privacyarchitectuur (PBD)	3	0	0	3	0	0	0
	Dataretentie (DRE)	2	1	0	1	0	0	0
	Verwijdering, vernietiging en anonimisering (DDA)	2	0	2	0	0	0	0
	Gebruik en beperking (URE)	3	3	0	0	0	0	0
Data toegang en data kwaliteit	Data-toegangsverzoeken (DAR)	4	3	1	0	0	0	0
	Data correctie verzoeken (DCR)	4	3	1	0	0	0	0
	Data verwijdering verzoeken (DDR)	4	4	0	0	0	0	0
	Data overdracht verzoeken (DPR)	4	4	0	0	0	0	0
	Nauwkeurigheid en volledigheid van gegevens (ACD)	2	0	1	1	0	0	0
Openbaren	Openbaarmaking en registratie door derden (TPD)	1	0	1	0	0	0	0
	Derdenovereenkomsten (TPA)	3	1	2	0	0	0	0
	Gegevensoverdracht (DTR)	Deze beheersdoelstelling is buiten scope geplaasts.						
Dataveiligheid	Informatiebeveiligingsprogramma (ISP)	7	0	5	1	1	0	0
	Identiteits- en toegangsbeheer (IAM)	1	0	0	1	0	0	0
	Veilige verzending (STR)	1	0	1	0	0	0	0
	Encryptie en eindpuntbeveiliging (ENC)	4	0	0	0	0	0	4
	Logging van toegang (LOG)	1	1	0	0	0	0	0
Monitoring en handhaving	Herziening van privacy-compliance (REV)	1	0	0	1	0	0	0

	Periodieke monitoring van privacy-controles (MON)	3	0	0	2	0	0	1
Totaal		104	28	43	17	9	0	7

H = Helemaal, G = Grotendeels, D = Deels, N = niet, n/a = nvt & NI = niet ingevuld.

Bijlage III Cross referenties GDPR elementen

Cross referentie tussen GDPR key elementen en GDPR artikelen. De volgende tabel toont de relatie tussen de GDPR key elements en de artikelen van de GDPR.

GDPR key element	GDPR artikel	Link naar online informatie
Privacyprincipes	5	https://gdpr-info.eu/art-5-gdpr/
Rechtmatigheid van verwerking	6	https://gdpr-info.eu/art-6-gdpr/
Voorwaarden voor toestemming	7	https://gdpr-info.eu/art-7-gdpr/
Rechten van de betrokkene	12-19	https://gdpr-info.eu/art-12-gdpr/ https://gdpr-info.eu/art-13-gdpr/ https://gdpr-info.eu/art-14-gdpr/ https://gdpr-info.eu/art-15-gdpr/ https://gdpr-info.eu/art-16-gdpr/ https://gdpr-info.eu/art-17-gdpr/ https://gdpr-info.eu/art-18-gdpr/ https://gdpr-info.eu/art-19-gdpr/
Recht op gegevensportabiliteit	20	https://gdpr-info.eu/art-20-gdpr/
Privacy door ontwerp / standaard	25	https://gdpr-info.eu/art-25-gdpr/
Verantwoordelijkheden van de verantwoordelijke en verwerker	24, 28	https://gdpr-info.eu/art-24-gdpr/ https://gdpr-info.eu/art-28-gdpr
Registratie van verwerkings-activiteiten	30	https://gdpr-info.eu/art-30-gdpr/
Beveiliging van de verwerking	32	https://gdpr-info.eu/art-32-gdpr/
Schending persoonsgegevens	33, 34	https://gdpr-info.eu/art-33-gdpr/ https://gdpr-info.eu/art-34-gdpr
Gegevensbeschermings-effectbeoordeling (DPIA)	35	https://gdpr-info.eu/art-35-gdpr/
Functionaris gegevens bescherming (DPO)	37, 39	https://gdpr-info.eu/art-37-gdpr/ https://gdpr-info.eu/art-39-gdpr
Overdracht van persoonsgegevens naar derde landen of internationale organisaties	44-50	https://gdpr-info.eu/art-44-gdpr/ https://gdpr-info.eu/art-45-gdpr/ https://gdpr-info.eu/art-46-gdpr/ https://gdpr-info.eu/art-47-gdpr/ https://gdpr-info.eu/art-48-gdpr/ https://gdpr-info.eu/art-49-gdpr/ https://gdpr-info.eu/art-50-gdpr/