DPO-Connect

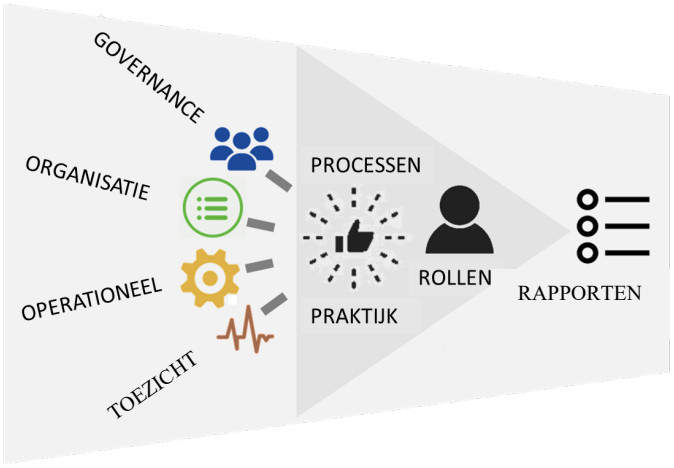
Het versterken van de communicatie en de samenwerking tussen DPO's en de GBA d.m.v. een digitaal platform

Handboek: Hoe een GDPR-compliance programma ontwikkelen?

Florence de Villenfagne et Patrick Soenen

Co-funded by the European Commission

Dit verslag werd gefinancierd door het programma Rechten, gelijkheid en burgerschap van de Europese Unie (2014-2020). De inhoud van dit verslag weerspiegelt uitsluitend de mening van de auteurs en valt uitsluitend onder hun verantwoordelijkheid. De Europese Commissie aanvaardt geen enkele verantwoordelijkheid voor het gebruik dat eventueel wordt gemaakt van de informatie die het bevat.



Hoe een GDPR-compliance programma ontwikkelen?

Deliverable D.3.2

Onderdeel opgesteld door DPO-pro in het kader van het Europese project DPO-Connect[1]

3 juni 2022

Auteurs : Florence de Villenfagne en Patrick Soenen

DPO-Connect is een project dat wordt medegefinancierd door de Europese Commissie (DG JUST) in het kader van het programma Rechten, gelijkheid en burgerschap van de Europese Unie (2014-2020).

Partners DPO-Connect : De Belgische Gegevensbeschermingsautoriteit (GBA), de Beroepsvereniging van DPO's van België (DPO-pro) en de Vrije Universiteit Brussel (VUB)

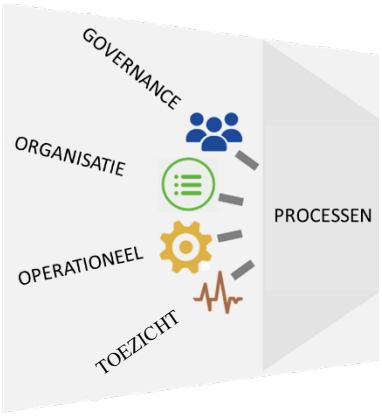
[1] De inhoud van deze publicatie weerspiegelt alleen de mening van de auteurs. het is op geen enkele manier een officieel standpunt van de Europese Commissie, DPO-pro of de andere partners van het DPO-Connect-project. De Europese Commissie en de auteurs aanvaarden geen enkele verantwoordelijkheid voor het gebruik dat eventueel wordt gemaakt van de informatie die het bevat.

Voorwoord

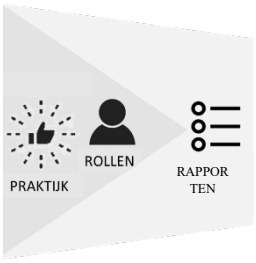
Wanneer een jurist en een auditor, beiden gespecialiseerd in gegevensbescherming, samen een studie schrijven over een GDPR-complianceprogramma, is het resultaat creatief en onvermijdelijk verschillend van wat men gewoonlijk kan lezen over de naleving van de GDPR door juristen of beveiligingsexperten afzonderlijk.

Het idee van deze deliverable is om, met een frisse en praktische blik, om de zaken te benaderen vanuit het oogpunt van de interne verantwoordelijkheden en op die manier organisaties concreet te kunnen helpen bij het structureren van hun naleving van de GDPR. De Algemene Verordening Gegevensbescherming (AVG of GDPR) is een zeer algemene wetgeving, die organisaties dan ook niet makkelijk praktisch kunnen toepassen. Aangezien organisaties hun activiteiten in processen structureren door rollen en verantwoordelijkheden van de verschillende actoren vast te leggen, is deze publicatie erop gericht om de vereisten van de verordening om te zetten in processen, vergezeld van verantwoordelijkheidsmatrixen en hierbij de aldus gegenereerde rapporten te specificeren.

Wie is verantwoordelijk voor de acties? Wie moet er optreden? Wie zal hulp en advies geven en wie moet absoluut geïnformeerd worden, zodat de GDPR uiteindelijk op een doeltreffende en duurzame manier wordt toegepast? En welke noodzakelijke rapporten/output leverde deze oefening op? Dit zijn de vragen die we hebben proberen te beantwoorden.



Het referentiekader voor het proces is ontleend aan de werkzaamheden van de GDPR-werkgroep van het IFACI (Institut Français de l'Audit et du Contrôle Interne)[2], met hun welwillende toestemming.



De praktijken, verantwoordelijkheidsmatrixen en output werden ontwikkeld in het kader van deze publicatie.

We vonden veel literatuur met de uitleg van de GDPR, de uiteenzetting van de principes, de verduidelijking van de verplichtingen. Maar we vonden nog geen uiteenzetting vanuit de gebruikelijke rollen en verantwoordelijkheden in organisaties.

Uiteraard is ons werk voor verbetering vatbaar en kunnen wij de volledigheid van de resultaten niet garanderen. In toepassing van de Plan-Do-Check-Act-methodologie die ons aan het hart ligt, zouden we graag uw constructieve feedback ontvangen in de hoop deze studie te perfectioneren. Intussen hopen we dat ons werk nuttig voor u zal zijn.

De auteurs

Florence de Villenfagne *Patrick Soenen*

[2] Cf. *Maîtriser et auditer les risques liés au GDPR*, **Groupe de travail RGDP de l'IFACI**, 2021, alleen beschikbaar voor IFACI-leden. De werkgroep was samengesteld uit Qadir Abdul, Valérie Bonnel, Pascale Chabrillat-Trahin, Maud Choquenet, Gilles Le Beux, Marjorie Mengeaud en werd geanimeerd door Patrick Soenen.

Inhoudsopgave

1. Doelstelling en toepassingsgebied

Het doel van de publicatie is om alle algemene acties op te lijsten, die een organisatie zou moeten implementeren om aan de GDPR te voldoen, vanuit de rollen en verantwoordelijkheden van de actoren van de organisatie en de uit te voeren onderdelen.

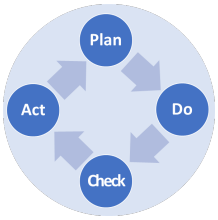
De Algemene Verordening Gegevensbescherming (hierna de "GDPR" of "Verordening") de voorschriften voor de bescherming van persoonsgegevens. De richtlijnen van het Europees Comité voor gegevensbescherming (EDPB) geven duidelijkheid over het begrip van de vereisten, maar leggen niet uit hoe deze vereisten op een praktische manier kunnen worden geïmplementeerd3.

In deze publicatie wordt een reeks processen voorgesteld, gestructureerd in 4 domeinen: Governance, Organisatie, Operationeel (beheer) en Toezicht. (Goede) praktijken[4] worden voorgestel voor elk proces, dat binnen de organisatie moet worden geïmplementeerd. Elke praktijk dient vervolgens opgesplitst te worden in verschillende taken, die nodig zijn voor de implementatie ervan. Deze taken kunnen wij niet uitwerken in deze bijdrage. Zij moeten vastgelegd worden naar gelang de omvang van de verwerking van persoonsgegevens, de activiteitensector, de omvang en de interne structuur van de organisatie, etc.

Deze publicatie houdt geen rekening met de specifieke kenmerken die voortvloeien uit de nationale wetgeving, noch met de verschillen naar gelang de specifieke activiteitensectoren, zoals bijvoorbeeld gezondheidszorg, die de verwerking van een grote hoeveelheidaan bijzondere categorieën van persoonsgegevens met zich meebrengen.

De naleving van de GDPR is een recente ontwikkeling in organisaties. De implementatie ervan wordt idealiter geïntegreerd in en gericht op de bestaande governance- en controlestructuren en -mechanismen. De impact ervan op data governance, risicobeheer en informatiebeveiliging is aanzienlijk en een voortdurende afstemming op de regelgevingseisen is van essentieel belang.

Naast de implementatie van compliance moet de duurzaamheid ervan in de loop van de tijd worden verzekerd. In lijn met de Deming-cyclus is continue verbetering gebaseerd op 4 activiteiten:



- De planning (Plan), met de omschrijving van het uit te voeren werk;
- De uitvoering (Do), het uitvoeren van de activiteiten;
- De controle (Check), die ervoor zorgt dat de activiteiten worden uitgevoerd zoals gepland;
- De actie (Act), waarbij de uitvoering van de activiteiten bijgesteld wordt.

2. Doelgroep

Deze gids is voornamelijk bedoeld voor Data Protection Officers (DPO's) of gelijkgestelde personen, maar ook voor iedereen die betrokken is bij de implementatie van de GDPR.

[3] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG

[4] In dit document begrijpen we onder *'praktijken' ('best practices - goede praktijken')*, de acties die nodig zijn om het doel van het proces te bereiken.

3. Rollen en verantwoordelijkheden

Voor elk proces en voor elke praktijk - een actie die bijdraagt tot het bereiken van de procesdoelstelling - wordt een verantwoordelijkheidsmatrix voorgesteld met gebruikmaking van een RASCI-model met de volgende definities:

- ***R - Responsible* (Verantwoordelijke)**: De rol, die het werk verricht om de activiteit te volbrengen. Een of meer rollen kunnen het werk uitvoeren.
- ***A - Accountable* (Eindverantwoordelijke)**: De rol, die de activiteit valideert, verantwoording aflegt en verantwoordelijkheid neemt. Elke praktijk heeft één persoon die "eindverantwoordelijk" is en die niet dezelfde als de Verantwoordelijke(n) is.
- ***C - Consulted* (Geraadpleegd)**: De rol(en) die wordt(worden) geraadpleegd en die informatie verstrekt (verstrekken).
- ***I - Informed* (Geïnformeerd)**: De rol(en) die op de hoogte wordt(worden) gehouden van de resultaten van de activiteiten.
- **S - *overSight* (Toezicht)**: De rol(en) die de uitvoering van activiteiten en/of de naleving van regelgeving verifieert (verifiëren).

Voor organisaties die uitgebreide bestuurs- en controlestructuren hebben, worden praktijken voorgesteld die specifiek zijn voor deze structuren. Organisaties die niet over deze specifieke functies beschikken, zullen moeten bepalen welke rol de verantwoordelijkheden zal hebben.

De volgende rollen zijn opgenomen in de verantwoordelijkheidsmatrixen:

Rol	Beschrijving
INTERNE ACTOREN	
Verwerkingsverantwoordelijke (VV)	De natuurlijke persoon of rechtspersoon, de overheidsinstantie, de dienst of een ander orgaan die het doel en de middelen voor de verwerking vaststelt. [5]
Bestuursorgaan	Dit orgaan, vaak de raad van bestuur genoemd, streeft op duurzame wijze naar waardecreatie door de strategie van de onderneming te bepalen, door doeltreffend, verantwoordelijk en ethisch leiderschap en door toezicht te houden op de prestaties van de onderneming. Het keurt het, door het uitvoerend management voorgestelde, kader voor interne controle en risicobeheer goed en evalueert de implementatie van dit kader.[6]
Uitvoerend management[7]	• Is belast met het operationeel beheer • Zorgt voor de totstandkoming van interne controles op basis van het door het bestuursorgaan goedgekeurde kader • Legt de jaarrekening voor en bereidt hun wettelijke publicatie voor

[5] Zie de definitie in het artikel 4 (7) van de GDPR
[6] Zie *Belgische Corporate Governance code*, Principe 2 Raad - Strategie - Toezicht, **Commissie Corporate Governance**, 2020, (https://www.corporategovernancecommittee.be/assets/pagedoc/200979066-1651062167_1651062167-belgische-corporate-governance-code-2020.pdf - geraadpleegd op 3 juni 2022)
[7] Zie *Belgische Corporate Governance code*, Principe 2 Uitvoerend management, **Commissie Corporate Governance**, 2020, *op.cit*.

Rol	Beschrijving
	• Verstrekt het bestuursorgaan de benodigde informatie voor de uitoefening van zijn verantwoordelijkheden • Legt verantwoording af aan het bestuursorgaan
Auditcomité	Dit comité staat het bestuursorgaan bij in het waarborgen van de juistheid en de getrouwheid van de rekeningen evenals van de geschiktheid en doeltreffendheid van de systemen voor interne controle en risicobeheer van de organisatie. Het comité volgt de interne audit en de externe controle op. Het auditcomité of "audit- en risicobeheerscomité" wordt opgericht door het bestuursorgaan.
Functionaris voor gegevensbescherming / Data Protection Officer (DPO) of Privacy Officer (PO)	De DPO is verantwoordelijk voor het informeren en adviseren van de verwerkingsverantwoordelijke, die hem heeft aangesteld, over zijn verplichtingen in het kader de GDPR. Het heeft ook een rol bij het toezicht op de naleving van de verordening. Hoewel de DPO een in de GDPR gedefinieerde rol is, is de Privacy Officer of Privacy Functionaris een niet- officiële rol, die niet door de verordening is gedefinieerd. Indien de verwerkingsverantwoordelijke op grond van de GDPR verplicht is om een DPO aan te stellen, kan hij hem alleen "DPO" noemen en dient deze de functies en taken uit te oefenen, zoals door de GDPR vastgelegd. Wanneer de verwerkingsverantwoordelijke deze verplichting niet heeft, kan hij er toch voor kiezen een persoon aan te duiden om toezicht te houden op en advies te geven over de naleving van de GDPR. Hij kan hem "PO" noemen of nog anders. De PO kan dan gelijkaardige functies invullen dan deze van een DPO of slechts een deel ervan, naargelang de beslissing van de Verwerkingsverantwoordelijke. Als de Verwerkingsverantwoordelijke niet verplicht is om een DPO aan te stellen, maar er toch een aanwijst door hem de naam "DPO" te geven, moet hij voldoen aan alle criteria die de GDPR voor de DPO oplegt (artikelen 37 en volgende van de GDPR).
GDPR-contactpersoon	Medewerker, die op een afdeling kan worden aangesteld om de informatie van de DPO door te geven aan werknemers, hen te adviseren, dagelijks te zorgen voor naleving van de voorschriften van de GDPR, het actieplan toe te passen en verzoeken of incidenten aan de DPO te melden. Andere benamingen bestaan ("data steward", "privacy contactpunt" ...). We gebruiken zelf de definitie van "GDPR-contactpersoon".
Hoofd informatiebeveiliging / Chief Information Security Officer (CISO)	De verantwoordelijke persoon voor de uitvoering van het informatiebeveiligingsbeleid en het toezicht daarop. De namen beveiligingsadviseur, beveilingsconsulent of Chief Information Security Officer (CISO) worden gebruikt.

Rol	Beschrijving
Gegevensverwerkingsafdeling (GV Afdeling)	Elke afdeling die persoonsgegevens verwerkt in het kader van haar operationele activiteiten.
Juridische dienst	Afdeling verantwoordelijk voor de juridische kewsties van een organisatie. Sommige organisaties stellen de DPO aan binnen de juridische dienst.
IT-afdeling (IT)	De IT-afdeling is verantwoordelijk voor het beheer van de informatiesystemen van de organisatie. Deze afdeling is verantwoordelijk voor het definiëren van de architectuur van het informatiesysteem, het ontwerpen, installeren en implementeren en exploiteren van het informatiesysteem. In dit kader is zij vaak betrokken bij het bedenken van oplossingen voor de verwerking van persoonsgegevens. Deze functies zijn onverenigbaar met die van de DPO.
***Project Management Office* / Project Bureau (PMO)**	De organisatiestructuur die de sturing en de ondersteuning van het beheer van projecten, programma's en projectportfolio's van de organisatie geheel of gedeeltelijk centraliseert.
Human Ressources / Personeelsdienst (HR)	Personeelsdiensten zijn onderverdeeld in twee hoofdactiviteiten, enerzijds de administratieve kant van personeelsbeheer waaronde salarisadministratie, juridische ondersteuning, arbeidscontracten... en anderzijds de ontwikkeling van het menselijk potentieel, waaronder loopbaanbeheer, vaardigheden- en prestatiebeheer, werving, opleiding
Interne Controle (IC)	In organisaties waar die bestaat, is Interne Controle verantwoordelijk voor de invoering en het beheer van een intern controlesysteem dat alle middelen, gedragingen, procedures en acties omvat, die bijdragen tot de beheersing van de activiteiten, de doeltreffendheid van de verwerkingen en het efficiënte gebruik van middelen.[8]. Interne controle moet op passende wijze rekening houden met materiële risico's, ongeacht of deze operationele, financiële en nalevingsrisico's zijn.
Compliance Officer	Deze rol beheert en houdt toezicht op de naleving van wet- en regelgeving binnen de organisatie. Het inventariseert de toepasselijke wet- en regelgeving. Hij/zij moet ervoor zorgen dat de medewerkers en de ondersteunende actoren deze voorschriften kennen, zodat zij deze op een doeltreffende manier kunnen naleven. Hij/zij rapporteert aan het management, de toezicht-houder en de autoriteiten. Hij/zij beantwoordt de vragen van de toezichthouder, voor wie hij/zij het eerste aanspreekpunt is.

[8] De basisreferentie is het COSO (Amerikaans interne controlekader gestructureerd in 5 componenten). Deze rol bestaat vooral in grote multinationals, de financiële sector..., maar zelden in een KMO.

Rol	Beschrijving
Risicomanager (*Risk Manager*)	De risicomanager helpt de organisatie bij het identificeren van haar risico's. Ter ondersteuning van het beheer draagt deze bij aan de verzekering en beheersing van deze risico's. Deze verschaft de medewerkers de methodologie voor het beoordelen van risico's en ondersteunt hen bij de toepassing van de methodologie, verzamelt informatie, valideert en rapporteert aan het management. Hij/zij beoordeelt het risico zelf niet.
Interne Audit (IA)	De onafhankelijke en objectieve activiteit om de nodige zekerheid te verschaffen dat risico's onder controle zijn en om verbeteringen in de werking van de organisatie voor te stellen.
EXTERNE ACTOREN	
Gegevensbeschermingsautoriteit (GBA)	Toezichthoudende autoriteit, onafhankelijke overheidsinstantie die verantwoordelijk is voor het toezicht op de toepassing van de GDPR, en zodoende de fundamentele rechten en vrijheden van natuurlijke personen ten aanzien van de verwerking te beschermen en het vrije verkeer van persoonsgegevens binnen de Unie te vergemakkelijken[9].
Betrokkene (Data Subject)	Geïdentificeerde of identificeerbare natuurlijke persoon[10], op wie de persoonsgegevens betrekking hebben
Verwerker (Processor)[11]	De natuurlijke of rechtspersoon, overheidsinstantie, dienst of andere instantie, dewelke ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.
Subprocessor	De Verwerker van een verwerker *(subprocessor)* die persoonsgegevens verwerkt in opdracht van Verwerkingsverantwoordelijke, maar op basis van een met Verwerker (*processor*) gesloten overeenkomst.

[9] Zie artikel 51 (1) van de GDPR
[10] Zie de definitie bij artikel 4 (1) van de GDPR
[11] Zie de definitie bij artikel 4 (8) van de GDPR

4. Het Model van de drie verdedigingslinies (Three Lines of Defense-model)

In organisaties met controlestructuren helpt het model van de drie verdedigingslinies organisaties bij het identificeren van de optimale structuren en processen om hun doelstellingen te bereiken, en hun governance- en risicobeheer te versterken, ook met betrekking tot het beheer van persoonsgegevens.

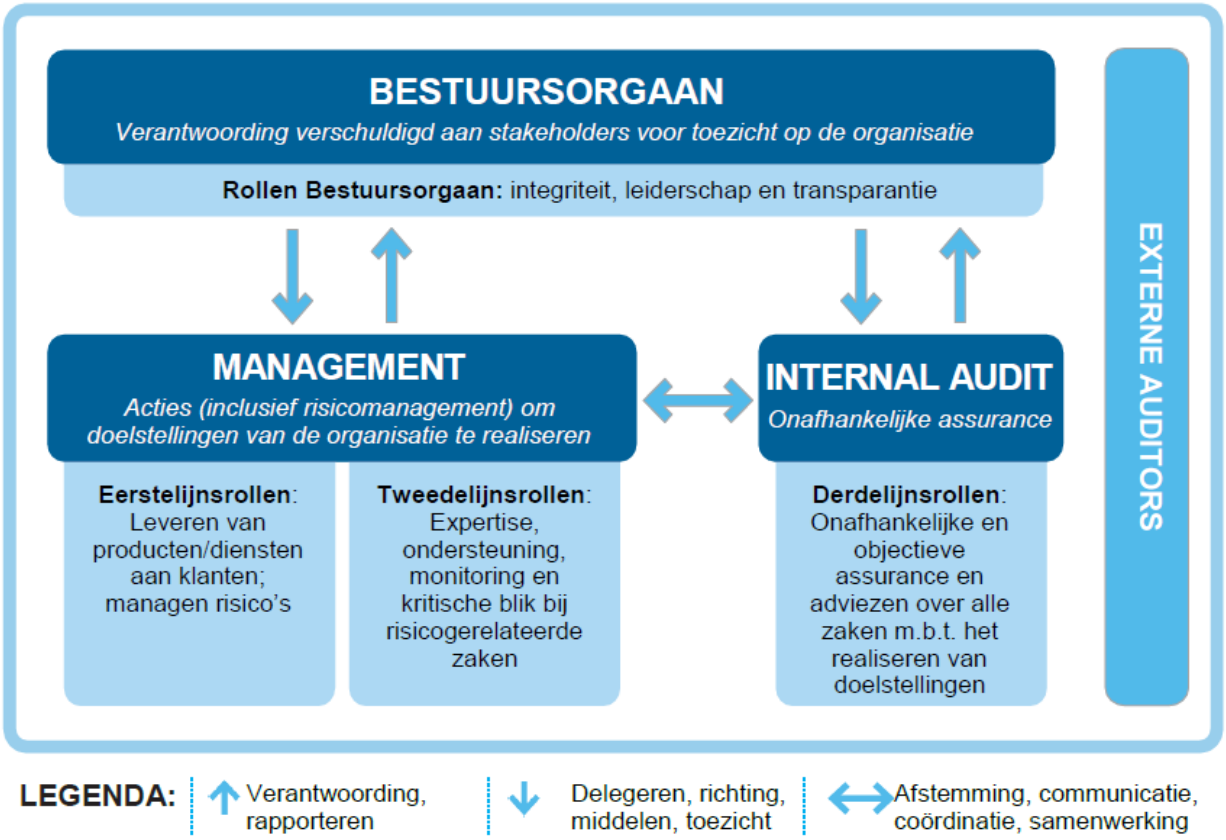


Schéma 1 - Three Lines Model van het IIA[12]

De governance van een organisatie stoelt op passende structuren en processen m.b.t. het beheer van persoonsgegevens, die bestuursorganen in staat stellen hun verantwoordingsplicht te vervullen, die het management toelaat de nodige maatregelen te nemen om deze doelstellingen te verwezenlijken op basis van risicoanalyse en beschikbare middelen, naast een onafhankelijke auditfunctie.

In de aanpak worden met name specifieke taken en verantwoordelijkheden voor elke verdedigingslinie vastgelegd:

- Controleactiviteiten, gedefinieerd en uitgevoerd door operationeel personeel, om onder meer risico's op dagelijkse basis te beheersen;
- Een systeem, gestructureerd en gecoördineerd door de tweede verdedigingslinie, bestaande uit de functionele afdelingen, verantwoordelijk voor de expertisegebieden en uit de functies, bedoeld om leiding te geven aan het algemene risicobeheersysteem (risicobeheerfuncties, interne controle, compliance, DPO, CISO[13], kwaliteitsverantwoordelijke...);

[12] Cf. *Het Three Lines Model van het IIA*, **The Institute of Internal Auditors**, 2020.
[13] Hoofd informatiebeveiliging (CISO)

- Een alomvattende en onafhankelijke controle door de derde verdedigingslinie, uitgevoerd door de onafhankelijke interne auditfunctie op het hoogste niveau van de organisatie.

5. De GDPR-processen

De uitvoering van een GDPR-complianceprogramma vereist het opzetten van processen door alle relevante belanghebbenden, met het oog op een gestructureerde aanpak die de verschillende eisen van de GDPR omvat. Deze processen worden opgedeeld in 4 domeinen[14] :

A. Governance	B. Organisatie	C. Operationeel beheer	D. Toezicht
Rollen en verantwoordelijkheden, sturende organen, beleidsmaatregelen en richtlijnen voor een adequaat beheer van de bescherming van persoonsgegevens binnen de organisatie.	Maatregelen en processen die moeten worden toegepast om aan de eisen van de GDPR-verordening te voldoen.	Processen en procedures die moeten worden uitgerold om de bescherming van persoonsgegevens operationeel te maken overeenkomstig de GDPR.	Mechanismen voor toezicht, follow-up, evaluatie en controle van het ingevoerde systeem, overeenkomstig de voorschriften van de GDPR-verordening en de bijbehorende richtlijnen. Het toezicht moet ervoor zorgen dat het systeem werkt zoals vooropgesteld. Hierdoor wordt de doeltreffendheid van het risicobeheer in de loop van de tijd verzekerd.

Tabel 2 - GDPR-procesdomeinen

De 4 gebieden worden in 21 processen uitgesplitst:

A. Governance

- A1. Verbintenissen van de Verwerkingsverantwoordelijke (VV)
- A2. Gegevensbeschermingsbeleid
- A3. Governance-organen, rollen en verantwoordelijkheden
- A4. Functionaris voor gegevensbescherming (DPO)

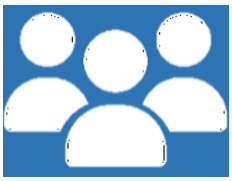
[14] De structuur is gebaseerd op die welke in de publicatie is ontwikkeld: *Controlling and auditing RGPD risks*, **IFACI RPGD Working Group**, 2021. Document alleen beschikbaar voor IFACI-leden.

B. Organisatie
B1. Rechtmatigheid van de verwerking (wettelijke basis en finaliteit)
B2. Register van verwerkingsactiviteiten
B3. Gegevensbeschermingseffectbeoordeling (DPIA)
B4. Gegevensbescherming door ontwerp en door standaard-instellingen (« Data protection by Design/Default »)
B5. Gebruik en bewaartermijn van persoonsgegevens
B6. Beheer van de verwerkers
B7. Transfers buiten de Europese Economische Ruimte (EER)
C. Operationeel domein
C1. Aansturing en uitvoering
C2. Rechten van de betrokkene
C3. Informatie en transparantie
C4. Bewustmaking en opleiding
C5. Businesscontinuïteitsbeheer (BCP)
C6. Beheer en melding van inbreuken in verband met persoonsgegevens
C7. Bescherming en beveiliging van persoonsgegevens
D. Toezicht en controle
D1. Toezicht en herziening (door de DPO)
D2. Herziening van de GDPR-maatregelen (door de actoren van de verdedigingslinies)
D3. Controle door de Gegevensbeschermingsautoriteit (GBA)

Tabel 3 - Domeinen en processen

Voor elk proces worden (goede) praktijken voorgesteld om aan de eisen van de GDPR *te voldoen. Elke praktijk* moet vervolgens *opgesplitst* worden *in een aantal taken* die *nodig zijn om ze te verwezenlijken. Deze taken zijn niet in dit document opgenomen. Zij moeten* inderdaad *worden* uitgewerkt *naar gelang van de omvang en de interne structuur van de organisatie,* de omvang *van de verwerking van persoonsgegevens, de sector waarin zij werkzaam is, enz.*

A. Governance domein



De rollen en verantwoordelijkheden, de bestuursorganen, het beleid en de richtlijnen maken een adequaat beheer van de bescherming van persoonsgegevens binnen de organisatie mogelijk.

A1. Verbintenissen van de Verwerkingsverantwoordelijke (VV)

De uitvoering van een doeltreffend gegevensbeschermingsbeheer begint op het niveau van de bestuursorganen, met name het orgaan van bestuur en de directie.

Matrix voor goede praktijken en verantwoordelijkheid:

Het dagelijks bestuur verwijst naar de rol die de praktijken uitvoert (R).

Rollen / **Praktijken**	**(VV) Verwerkings-verantwoordelijke**	**[D]PO**
De vaststelling van de verplichting een DPO aan te stellen	A	
Het aanstellen van een Data Protection Officer (DPO) overeenkomstig de vereisten van de GDPR (onafhankelijkheid, afwezigheid van belangenconflicten ...) of een privacyfunctionaris (Privacy Officer - PO)[15]	A	
De toewijzing van de nodige middelen zodat de [D]PO in staat is zijn/haar verantwoordelijkheden op passende wijze uit te oefenen met het oog op de naleving van de RGPD	A	C/I
De [D]PO een passende positie geven in de organisatiestructuur, met toegang tot (en rechtstreekse rapportage aan) bestuursorganen en met de autoriteit om zijn/haar verantwoordelijkheden uit te oefenen	A	-
Het formaliseren van de aan de [D]PO toevertrouwde opdrachten: opdrachtbrief, geheimhoudingsverbintenis, budget, werklast, bescherming tegen elke bestraffing voor de uitvoering van zijn opdrachten, enz.	A	C/I
Het onderwerp van de gegevensbescherming op de agenda van de bestuursorganen zetten	A	C/I
Het op de hoogte houden van de [D]PO van de onderwerpen inzake gegevensbescherming, zoals besproken in de beheerscomités	A	I
In geval van gezamenlijke verwerkingsverantwoordelijkheid een overeenkomst tussen de gezamenlijke verantwoordelijke partijen ondertekenen.	A	C

[15] Zie de uitleg van het verschil tussen "DPO" en "PO" in afdeling 3 – Rollen en verantwoordelijkheden, waar de term "functionaris voor gegevensbescherming" wordt gedefinieerd.

Rapporten (Deliverables)

- Analyse van de aanstelling van een DPO
- Aanwijzing van de DPO door de bestuursorganen
- Aangifte bij de GBA
- Functionele beschrijving van de [D]PO
- Updaten van het organigram (met inbegrip van de rol van de DPO)
- Contract met de externe DPO of wijziging van de arbeidsovereenkomst van de interne DPO
- Budget voor de DPO
- Uittreksels uit de notulen van bestuursorganen en bijlagen, met betrekking tot de onderwerpen en de verwerking van persoonsgegevens
- Overeenkomst(en) m.b.t. gezamenlijk verwerkingsverantwoordelijkheid

A2. Gegevensbeschermingsbeleid

Art. 24.2

Het beheer van de gegevensbescherming en -beveiliging wordt vastgesteld a.d.h.v. passende beleidsmaatregelen, goedgekeurd door de directie en via de organisatiestructuren in de organisatie verspreid.

Matrix voor goede praktijken en verantwoordelijkheid:

Rollen / Praktijken	Bestuursorgaan	VV	[D]PO	CISO	HR	GV Afdeling
Een intern (algemeen) privacybeleid (of gelijkwaardig) vaststellen en uitvoeren, met de omschrijving van het beheer van de gegevensbescherming door de organisatie	A	R	C	C	C	
De goedkeuring van het intern beleid	A/R	R	C	C	C	
Het vaststellen en uitvoeren van het beleid inzake de bescherming van persoonsgegevens, de beveiliging van informatiesystemen (ISSP), charters voor het gegevensbeheer		A	C	R	R/I	
De publicatie en communicatie van het beleid van en aan de belanghebbenden		A	I	C	R/I	R/I
De integratie van de gegevensbescherming in arbeidsovereenkomsten en interne reglementen		A	C	-	R	I

Rapporten (Deliverables)

- Algemeen privacybeleid (governance)
- Beleid inzake de beveiliging van informatiesystemen (Information Systems Security Policy - ISSP), dat de visie van de verwerkingsverantwoordelijke op de beveiliging van informatiesystemen weerweerspiegelt
- Specifiek beleid inzake de gegevensbescherming en de informatiebeveiliging. Specifieke beleidsmaatregelen hebben betrekking op het correcte gebruik van IT-middelen, de classificatie van informatie, het beleid inzake veiligheidsmachtigingen, het beheer van wachtwoorden, het gebruik van internet, e-mail en sociale media, enz.
- Handvest inzake gegevensbeheer, met de beschrijving van de de verantwoordelijkheden en praktijken voor het beheer van gegevens, met als doel de kwaliteit, de integriteit, de beschikbaarheid en de beveiliging van de gegevens te waarborgen
- Communicatieplan voor charters en beleidslijnen
- Artikelen in de arbeidsovereenkomst en/of interne reglementen, die de verplichting inhouden om het beleid inzake de beveiliging en de bescherming van persoonsgegevens na te leven

A3. Bestuursorganen, rollen en verantwoordelijkheden

Art. 24

Bestuursorganen "zetten de toon" in de organisatie. Zij moeten er zich toe verbinden de regels inzake de gegevensbescherming na te leven en het belang van de gegevensbescherming benadrukken bij alle belanghebbenden die in aanraking kunnen komen met de gegevens.

Door de taken en verantwoordelijkheden op het gebied van gegevensbescherming door middel van duidelijke communicatiekanalen vast te stellen, kunnen alle niveaus van de organisatie passende praktijken toepassen.

Matrix voor goede praktijken en verantwoordelijkheid:

Rollen / **Praktijken**	Dagelijks Bestuur	VV	[D]PO	CISO	PMO	Interne Controle	Interne Audit
Het vaststellen van verantwoordelijkheids-matrixen voor de betrokken van de activiteiten m.b.t. de bescherming en beveiliging van persoonsgegevens.	R	A	C	C			
De integratie van de bescherming van de persoonsgegevens in bijvoorbeeld het:		A	C				
○ Bestuurs- of stuurcomités voor de projecten van de informatiesystemen					R		
○ Comités voor gegevensbeheer				R	R		
○ Terugkerende interne controleactiviteiten						R	
○ Auditwerkzaamheden							R
Het informeren van de bestuursorganen over de implementatie van de gegevensbescherming	A	I	R	C	C	C	C/(R)

Rapporten (Deliverables)

- Verantwoordelijkheidsmatrix (RACI)
- Uittreksels uit de notulen van de comités, met inbegrip van de bijlagen, met betrekking tot de onderwerpen en de verwerking van persoonsgegevens
- Mededelingen m.b.t. de naleving van de gegevensbescherming aan de bestuursorganen

A4. Functionaris voor gegevensbescherming (DPO)

Art. 37-39

Het vaststellen en aanduiden van de [D]PO of een "Generaal[16]" voor de bescherming van persoonsgegevens binnen de organisatie, die regelmatig verslag uitbrengt aan de verwerkingsverantwoordelijke.

Matrix voor goede praktijken en verantwoordelijkheid:

Rollen / Praktijken	VV	[D]PO	CISO	IT/PMO	GV Afdeling	Interne Controle Interne Audit	Betrokken	GBA
De mededelng van de contactgegevens van de DPO aan de toezichthoudende autoriteiten	A/R	I						I
De bekendmaking van de aanstelling van de DPO aan de belanghebbenden (zowel binnen als buiten de organisatie)	A/R		I	I	I	I		
De eventuele aanstelling van een GDPR-contactpersoon[17]		C	I	I	R	I		
De [D]PO toegang verschaffen tot alle informatie, die hij nodig heeft voor de uitvoering van zijn taken	A	I	R	R	R	R		
Het opstellen van een jaarverslag voor de bestuursorganen	A	R	C	C		C		
De actoren die persoonsgegevens verwerken informeren over vereisten van de GDPR	I	A/R	I	I	I	I		
Controle op de naleving van de GDPR	C/I	A/R	C/I	C/I	C/I	C/I		
Het adviseren van belanghebbenden over de bescherming van persoonsgegevens	I	A/R	I	I	I	I		
De samenwerking met de Gegevensbeschermingsautoriteit en het contactpunt voor betrokkenen	C/I	A/R	C/I	C/I	C/I	C/I	C/I	C/I

Rapporten (Deliverables)

- Kennisgeving van de aanstelling van de DPO aan de GBA
- Informeren van de belanghebbenden (intern en extern) over de benoeming van de DPOI
- Jaarverslag
- Advies van de DPO
- Programma voor toezicht op de naleving van de GDPR (zie ook D.1)

[16] Zie de uitleg over het verschil tussen een DPO en een PO in deel 3 - Taken en verantwoordelijkheden.
[17] Zie de definitie van deze rol in Afdeling 3 - Rollen en verantwoordelijkheden.

B. Organisatie

Maatregelen en processen die moeten worden uitgevoerd om aan de eisen van de GDPR-verordening te voldoen.

B1. Rechtmatigheid van de verwerking (wettelijke basis en finaliteit)

Art. 6

Alle persoonsgegevens moeten rechtmatig, eerlijk en transparant ten aanzien van de betrokkene worden verwerkt en voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en verwerkt. Hieronder volgen de praktijken in verband met wettigheid. Transparantie wordt verder verduidelijkt in punt C.3.

Matrix voor goede praktijken en verantwoordelijkheid:

Rollen / Praktijken	VV	[D]PO	CISO	IT/PMO	GV Afdeling
De vaststelling van rechtsgrond (of rechtmatigheidsgronden) en de doeleinden van elke verwerking van persoonsgegevens	A	C			R
Het verzamelen van de toestemming in overeenstemming is met de GDPR[18]	A	C	C/I	I/R	R
De organisatie van de bewaring van bewijzen van toestemming.	A	C	C/I	R	R
De documentatie van de wettelijke verplichting als rechtsgrond voor de verwerking	A	C			R
De rechtvaardiging van het algemeen belang als rechtsgrond voor de verwerking	A	C			R
De rechtvaardiging van het gerechtvaardigd belang als rechtsgrond voor de verwerking is ("drievoudige toets"[19])	A	C			R
De eventuele aanpassing van de verwerkingen om te voldoen aan de doeleinden en de rechtsgrond, en de stopzetting van niet-conforme verwerkingen	A	C		I/R	R

[18] Ook moet worden voorzien in de mogelijkheid om toestemmingen op verzoek van de betrokken personen in te trekken (zie punt C.2)
[19] Doel, noodzaak en wegingstoetsen

De toepassing van het minimaliseringsbeginsel bij het verzamelen van gegevens (afhankelijk van het doel van de verwerking). Zie ook B.4.	A	C		I/R	R

Rapporten (Deliverables)

- Inventaris van de verwerkingen, hun doel en de rechtsgronden
- Procedure voor het verkrijgen en het intrekken van toestemming en de bewaring van bewijsmateriaal
- (Model van) rechtvaardiging van het gerechtvaardigd belang
- (Model van) rechtvaardiging in het algemeen belang (indien van toepassing)

B2. Register van verwerkingsactiviteiten

Art. 30

De activiteiten in verband met de verwerking van persoonsgegevens worden geregistreerd in een register.

Matrix voor goede praktijken en verantwoordelijkheid:

Rollen / Praktijken	VV	[D]PO	GDPR-contactpersoon	GV Afdeling
Een inventaris maken van de bestaande verwerkingen van persoonsgegevens	A	R	C	C
Het aanmaken van het verwerkingsregister als "Verwerkingsverantwoordelijke" of als "Verwerker"	A	R	I	I
De vaststelling en toepassing van een procedure voor het bijwerken van het (de) register(s)	A	C	C	R
De bepaling van de noodzaak om verwerkingen in het register op te nemen (art. 30, lid 5, van de GDPR)	A	C	C	R
De toewijzing van de verwerkingingen aan het register als "Verwerkingsverantwoordelijke" of als "Verwerker"	A	R	I	
Het organiseren van de opleiding en eventuele ondersteuning van de GDPR-contactpersonen[20] .	A	C	R/C	R
Het verzamelen van alle informatie, nodig voor het register	A	C	C	R
Het uitwerken van een procedure voor regelmatige herziening van het register				

Rapporten (Deliverables)

- Inventaris van de gegevensverwerkingen en alle informatie daarover
- Register van de verwerkingsverantwoordelijke, met alle informatie krachtens artikel 30 van de GDPR – met bijwerkingen
- Register van de verwerker, met alle informatie krachtens artikel 30 van de GDPR – met bijwerkingen
- Procedure voor het bijwerken van het (de) register(s)
- Opleiding van GDPR-contactpersonen

[20] De contactpersonen moeten de departementen kunnen adviseren over de identificatie van de verwerkingen en helpen bij het verzamelen van de voor het register vereiste informatie

B3. Gegevensbeschermingseffectbeoordeling (DPIA)

Art. 35

Effectenbeoordelingen dienen daadwerkelijk worden uitgevoerd voor de geplande verwerkingen, met een waarschijnlijk groot risico voor de rechten en vrijheden van betrokkenen. Op die manier worden de risico's van een inbreuk op die rechten en vrijheden tot een minimum beperkt.

Matrix voor goede praktijken en verantwoordelijkheid:

Rollen / Praktijken	VV	[D]PO	GDPR-contactpersoon	CISO	GV Afdeling	Projectverant-woordelijke[21]	GBA
Het bepalen van de verwerkingen die in aanmerking komen voor een DPIA, op basis van artikel 35 van de GDPR en met name door toepassing van de criteria die zijn vastgesteld door de EDPB[22] en de bevoegde toezichthoudende autoriteiten (zoals de GBA).	A	R/C	C	R/C			
De vaststelling en uitvoering van een methodiek voor het uitvoeren van DPIA's	A/R	C					
Het eventuele selecteren van een instrument voor het uitvoeren van DPIA's en de invoering ervan	A	C/R	C	C	R	C	
De vaststelling van de planning voor de voltooiing van de DPIA's	A	C	C	C	R/C	C/I	
Het uitvoeren van de DPIA's[23] en de redactie van het verslag	A	C	I	R	R	R	
Het bepalen van de maatregelen om de risico's te beperken en indien nodig een actieplan opstellen	A	I	I	R	R	R	
De uitvoering en monitoring van het actieplan	A	R					C
De raadpleging van de GBA bij hoge restrisico's	A	R					C

Rapporten (Deliverables)

- Lijst van de verwerkingen die in aanmerking komen voor een DPIA
- DPIA-methodologie
- DPIA-instrument, mogelijks
- Planning van de uitvoering van DPIA's
- DPIA, met de volgende elementen per uitgevoerde analyse: voorstelling van de overwogen verwerking(en), lijst van uitgevoerde maatregelen, risicobeoordeling en in kaart brengen van de risico's, een gemotiveerde beslissing, eventueel het actieplan

[21] In het kader van de uitwerking van een nieuw project
[22] Europees Comité voor gegevensbescherming
[23] Voor een meer gedetailleerde studie van de stappen die bij de DPIA moeten worden doorlopen, zie de DPIA-gidsen van de CNIL, 2018, https://www.cnil.fr/fr/guides-aipd (geraadpleegd op 3 juni 2022)

- Actieplan en follow-up: maatregelen, verantwoordelijke personen, deadlines
- Advies van de GBA, wanneer geraadpleegd bij hoge restrisico's

B4. Gegevensbescherming door ontwerp en door standaard-instellingen (« *Data protection by Design/Default* »)

Art. 25

Het verzekeren, in het ontwerpstadium van de verwerkingen van persoonsgegevens, van de passende technische en organisatorische maatregelen of het overwegen hiervan, om de persoonsgegevens adequaat te beschermen en tot een minimum te beperken.

Matrix voor goede praktijken en verantwoordelijkheid:

Rollen / Praktijken	VV	[D]PO	GDPR-contactpersoon	CISO	IT/PMO	GV Afdeling	Projectverant-woordelijke	Stuurcomité
Het uitwerken van een procedure en/of methodologie voor de "gegevensbescherming by design/default" om de principes van de GDPR te waarborgen vanaf het ontwerp en door standaardinstallingen	A	I	I	I	R	I	I	I
De procedure integreren in de methodologie van het projectbeheer	A	C/I	C/I	I	R	I	I	I
De opleiding van projectmanagers en hoofdrolspelers in de methodologie	A	I	I	C	C	C/R	R	I
De toepassing van de methodologie in projecten met betrekking tot persoonsgegevens	A	I	I	I	I	I	I	R
De evaluatie van de resultaten van de “Data protection by Design/Default”[24]	A	I/C	I/C	R	I	R	R	C/I
Het bepalen van de acties die uitgevoerd moeten worden	A	I	I	R	I	R	R	I
De uitvoering en monitoring van het actieplan								

Rapporten (Deliverables)

- Procedure en methodologie voor de gegevensbescherming "by Design/Default"
- Opleidingsmateriaal over de aanpak en de procedure van "Data protection by Design/Default", eventueel geïntegreerd in het opleidingsmateriaal van de methodologie van het beheer van de projecten
- Notulen van de vergaderingen met de DPO m.b.t. de resultaten van de analyses "Data protection by Design/Default
- Actieplan van de uit te voeren maatregelen, per project
- Opvolging van de actieplannen: maatregelen, verantwoordelijken, deadlines

[24] Wanneer een nieuwe oplossing wordt ontworpen, is het een goede praktijk om met de DPO te overleggen over de juiste toepassing van de “Data protection by Design/Default”-beginselen. In het algemeen wordt een vergadering gepland met de ontwerpers (bv. IT, PMO) en de DPO, zodat de DPO kennis kan nemen van de analyse die in het kader van het project is uitgevoerd.

B5. Gebruik en bewaartermijn van persoonsgegevens

Art. 5.2 e)

Persoonsgegevens moeten worden gebruikt voor het doel waarvoor zij zijn verzameld en mogen vervolgens niet worden verwerkt op een onverenigbare wijze met dat doel. Zij mogen enkel bewaard worden, in een vorm die het mogelijk maakt de betrokkenen te identificeren voor een termijn, niet langer dan noodzakelijk voor de verwezenlijking van de doeleinden van de verwerking, tenzij bijkomende rechtvaardiging.

Matrix voor goede praktijken en verantwoordelijkheid:

Rollen / **Praktijken**	**VV**	**[D]PO**	**GDPR-contactpersoon**	**IT/PMO**	**GV Afdeling**
De inventarisatie van de (categorieën) persoonsgegevens die door de organisatie worden verwerkt - gerangschikt naar doel van de verwerking (uit het register)	A	C	C	I	R
Het bepalen van de bewaringstermijn voor gegevens volgens de noodzaak[25] (vaste duur of afhankelijk van het bereiken van een factor)	A	C	C	I	R
Het bepalen van wat er met de gegevens gebeurt na de vastgestelde bewaarperiode[26]	A	C	C	R/C	R
De toepassing van de vastgestelde bewaringstermijnen (in IT-systemen, in systemen voor de opslag van papieren documenten, in de organisatie van de toegang tot gegevens)	A	C	C	R/C	R
De Verwerkers instructies geven voor het toepassen van bewaartermijnen	A	C	C	R/C	R
Het verwerken van de informatie over de bewaartermijn in het verwerkingsregister (of een verwijzing naar deze informatie in het register)	A	C	C	-	C

Rapporten (Deliverables)

- Document(en) met de bewaartermijnen voor de gegevens, naar gelang van de doeleinden en de computersystemen waarin de gegevens zijn opgeslagen
- Uitvoeringsinstructies voor de verwerkers

[25] In overeenstemming met het minimalisatiebeginsel
[26] Verwijdering of bewaring voor een ander (rechtmatig) doel

B6. Beheer van de verwerkers

Art. 28

De activiteiten van de verwerkers en de daaropvolgende verwerkers (sub-processors) worden uitgevoerd voor de rekening van de verwerkingsverantwoordelijke. De verantwoordelijkheden en verplichtingen worden vastgelegd in een verwerkersovereenkomst overeenkomstig artikel 28 van de GDPR.

Matrix voor goede praktijken en verantwoordelijkheid:

Rollen / **Praktijken**	**VV**	**[D]PO**	**GDPR-contactpersoon**	**CISO**	**IT/PMO**	**GV Afdeling**	**Juridische dienst**
Het opstellen van model van verwerkers-overeenkomst met de clausules van artikel 28 van de RGPD (of gebruik van het Europese model)	A	C/R					R
Het opnemen in het model van het Bijzondere Lastenkohier van de bepalingen met betrekking tot de GDPR opnemen (alleen van toepassaing voor entiteiten onderworpen aan de regelgeving inzake overheidsopdrachten)	A	C	C/R			R	
De inventarisatie van de verwerkers en identificatie van de verwerkingsactiviteiten waarbij deze verwerkers betrokken zijn	A	C	C/R			R	C/R
De inventarisatie van de contracten met de verwerkers en de GDPR-clausules hierin	A	C		R		(R)	
Het vaststellen van de veiligheidsmaatregelen, op te leggen aan de verwerkers naar gelang van de aard van de gegevens die zij namens de VV verwerken, de risico's...	A	C	C/R	C		R	
Het toezicht op de garanties[27] die de verwerker biedt voor de naleving van de GDPR in het kader van de verwerking waarbij hij betrokken is, op de gegevens die hij namens de VV verwerkt en op het risico voor de rechten en vrijheden van de betrokkene	A	C	C			R	C

[27] De verwerkingsverantwoordelijke doet “uitsluitend een beroep op verwerkers die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking aan de vereisten van deze verordening voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd". Artikel 28, lid 1, GDPR.

Het afsluiten van verwerkersovereenkomsten	A	C					
De vaststelling van een procedure voor de controle en toezicht op de naleving van de verwerkersverplichtingen ("voldoende garanties"), (auditprogramma)	A	C	C/R			R	
De vaststelling van het land waar de gegevens door de verwerker worden verwerkt of van waaruit toegang tot de gegevens kan worden verkregen (vaststelling van de doorgifte naar derde landen - zie B.7)	A	C	C/R			R	
Het opnemen van de verwerkers in het register ("geadresseerden")	A	C	C/R			R	

Rapporten (Deliverables)

- Model van verwerkersovereenkomst - Artikel 28 RGPD (*Data processing Agreement)*
- Lijst van technische en organisatorische beveiligingsmaatregelen die afhankelijk van de omstandigheden (aard van de gegevens, risico's, stand van de techniek, kosten) aan de verwerker zouden kunnen worden opgelegd
- Inventaris van de verwerkers
- Inventarisatie van contracten met de verwerker en de hierin opgenomen gegevensbeschermingsclausules
- Inventaris van de transfers naar "derde landen" (zie B.7)
- Auditprogramma van de verwerkers

B7. Transfers buiten de Europese Economische Ruimte(EER)[28]

Hoofd-stuk V

Elke doorgifte van persoonsgegevens aan een derde land buiten de EER of aan een internationale organisatie moet voldoen aan de in de GDPR vastgestelde waarborgen.

Matrix voor goede praktijken en verantwoordelijkheid:

Rollen / Praktijken	VV	[D]PO	GDPR-contactpersoon	CISO	IT/PMO	GV Afdeling
De vaststelling van de doorgifte van persoonsgegevens aan "derde landen" (buiten de Europese Economische Ruimte) - zie B.6	A	C	C/R			R
De vaststelling of de gegevens naar een verwerker of een VV worden gezonden	A	C/R	C/R			C
Het bepalen van de garantie die de overdracht mogelijk maakt (land dat een adequate bescherming biedt[29], passende waarborgen die geen toestemming van de toezichthoudende autoriteit vereisen (standaardcontractbepalingen en aanvullende beschermingsmaatregelen; Bindende BedrijfsVoorschriften (Binding Corporate Rules))[30], passende waarborgen die wel toestemming van de toezichthoudende autoriteit vereisen (specifieke clausules...)[31] , afwijkingen voor specifieke situaties[32] , of dwingende gerechtvaardigde belangen [33]	A		C/R			R
Indien standaardcontractbepalingen worden gebruikt • Het uitvoeren van analyse van het overdrachtsrisico (DTIA)[34] en op basis van het resultaat eventueel aanvullende beschermingsmaatregelen nemen • Het verifiëren of de nieuwe standaardcontract-bepalingen van juni 2021 worden gebruikt[35] of dat het nog steeds de verouderde bepalingen zijn • Het gebruik van de nieuwe standaardcontractbepalingen voor alle nieuwe contracten vanaf 27 september 2021[36]	A	C	C/R	C		R C R

[28] De regels inzake gegevensbescherming gelden voor de Europese Economische Ruimte, die naast de landen van de Europese Unie ook IJsland, Liechtenstein en Noorwegen omvat. Zie: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_nl

[29] Artikel 45 GDPR

[30] Artikel 46, lid 2, GDPR

[31] Artikel 46, lid 3, GDPR

[32] Artikel 49 GDPR

[33] Artikel 49.1, alinea 2 GDPR

[34] TIA of DTIA - (gegevens)overdrachtseffectbeoordeling

[35] Https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32021D0914&from=FR (bekeken op 3 juni 2022)

[36] De oude clausules moeten vóór 27 december 2022 door de nieuwe modelcontractbepalingen worden vervangen

Rollen / Praktijken	VV	[D]PO	GDPR-contactpersoon	CISO	IT/PMO	GV Afdeling
• Het vastleggen van te gebruiken module bijd e toepassing van standaardcontractbepalingen worden gebruikt, moet de worden bepaald volgens het type overdracht (overdracht tussen een VV en een verwerker, tussen VV's, tussen verwerkers of tussen een verwerker en een VV)						

Rapporten (Deliverables)

- Lijst van overdrachten naar derde landen en de gebruikte waarborgen
- Inventaris van contracten waarin de oude standaardcontractbepalingen nog worden gebruikt
- DTIA-model
- DTIA bij gebruik van contractuele standaardclausules voor overdracht

C. Operationeel beheer

De uit te rollen processen en procedures om de bescherming van persoonsgegevens op een GDPR-conforme manier te operationeel te maken

C1. Sturing en uitvoering

Art. 24

Oprichting van een stuurgroep met de nodige middelen en vaardigheden voor de operationele uitvoering van het RGPD-systeem.

Matrix voor goede praktijken en verantwoordelijkheid:

Rollen / Praktijken	VV	[D]PO	GDPR-contactpersoon	CISO	IT/PMO	GV Afdeling
De vaststelling van een complianceprogramma m.b.t. de GDPR	A	R/S[37]	C/I	C/I	R	C/I
De aanwijzing van het team belast met het beheer van dit programma	A/R	I	I	I	I	I
Het stellen van de prioriteiten en het plannen van compliance-activiteiten	A	R/S[38]	C/I	C/I	R	C/I
Het aansturen van het netwerk van GDPR-contactpersonen voor de invoering van het compliancemechanisme	A	R	C	C	R	
Het organiseren van interne processen om de naleving van de gegevensbescherming te verzekeren	A	C/S	C	C	R/C	R
Het beheer van de risico's in verband met de verwerking van persoonsgegevens	A	C/S	C	C	C	R
De vaststelling van de indicatoren en dashboards voor het toezicht op de naleving van de RGPD	A	R/S	C/I	C/I	R	C/I

Rapporten (Deliverables)

- Programma voor GDPR-compliance
- Documentatie van het GDPR-programma: doelstelling, middelen, budget, deadlines, risico's, toezicht
- Notulen van de vergaderingen van de stuurgroep

[37] De CNIL verwijst naar de DPO als een piloot / dirigent. https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes, geraadpleegd op 3 juni 2022)
[38] Idem

- Beschrijven en bijwerken van processen en procedures
- Risico-register
- Indicatoren voor de opvolging
- Dashboard voor de opvolging van de uitvoering

C2. Rechten van de betrokkene

Art. 12-23

De verantwoordelijke voor de verwerking past de processen en de procedures toe, die de uitoefening van het recht van toegang, rectificatie, uitwissing, bezwaar en beperking van de verwerking mogelijk maken en die de gegevensoverdraagbaarheid van de betrokkene waarborgen.

Matrix voor goede praktijken en verantwoordelijkheid:

Rollen / Praktijken	VV	[D]PO	GDPR-contactpersoon	IT/PMO	GV Afdeling
De bepaling van de toepasselijke rechten (volgens de rechtsgronden)	A	C			R
Het aanmaken van een registrer van de verzoeken	A	R	C/R		C/R
De vaststelling van de procedures en de toepassing ervan om te reageren op de uitoefening van elk van de rechten, naar gelang van de categorie van betrokken personen[39]	A	S/C	C	C	R
Het bepalen van de maatregelen voor de authenticatie van aanvragers	A	S/C	C		R
Het inventoriëren van de de systemen waarin persoons-gegevens worden verzameld en te bepalen hoe in elk systeem aan het verzoek kan worden voldaan	A	S/C	C	R/C	R/C
Het vastleggen van een procedure om, in geval van een verzoek tot gegevenswissing, na te gaan of de gegevens inderdaad kunnen worden gewist, en zo nodig de wissing uitvoeren.	A	S/C	C	R/C	R/C
De opleiding van het personeel die de verzoeken tot uitoefening van rechten behandelt (frontoffice, ondersteunende dienst, enz.)	A	S/C	C		R
De vaststelling van de procedure voor de behandeling van een klacht	A	S/C	C		R
Het opstellen van sleutelindicatoren en/of verslagen voor analyse en monitoring van verzoeken	A	R	C/I		C/I

[39] In voorkomend geval, implementatie van een Self Service-portaal voor de betrokkenen

Rapporten (Deliverables)

- Procedure, per categorie van betrokkenen (klanten /burgers /patiënten /werknemers /leveranciers), voor het beheer van elk toepasselijk recht
    - Toegang (met inbegrip van het vrijgeven van informatie en het kopiëren van gegevens)
    - Verbetering
    - Verwijdering
    - Recht om te worden vergeten
    - Beperking van de verwerking
    - Overdraagbaarheid
    - Verzet
    - Intrekking van de toestemming
    - Geautomatiseerde individuele beslissing
- Procedure voor de authentificatie van de persoon die om de uitoefening van zijn rechten verzoekt
- Inventaris van de systemen met de modaliteiten voor het uitvoeren van de zoekopdrachten
- Procedure voor het beheer van klachten
- Opleidingsmateriaal voor het personeel
- Toezichstindicatoren en verslagen

C3. Informatie en transparantie

Art. 12-14

Er moeten passende maatregelen worden getroffen om de betrokkenen de nodige informatie te verstrekken over de verwerking van hun persoonsgegevens.

Matrix voor goede praktijken en verantwoordelijkheid:

Rollen / Praktijken	VV	[D]PO	GDPR-contactpersoon	HR	GV Afdeling
Het bepalen van de categorieën van betrokkenen, die moeten worden geïnformeerd	A	C	C	R	R
Het bepalen van de geschikte kanalen voor het inzamelen ed de communicatie met deze betrokkenen (website, intranet, intern handvest, bijlage bij de arbeidsovereenkomst, arbeidsreglement, enz.)	A	C	C	R	R
Het identificeren, per categorie van betrokkenen, van de verwerkingen, die op hen betrekking hebben (op te halen uit het register)	A	C	C	R	R
Het opnemen van de bewaringstermijn in de informatie aan de betrokkene	A	C	C	R	R
Het opstellen van een "privacyverklaring" of een "privacy-handvest", die de informatie van artikel 13 of 14 van de GDPR bevat	A	C	C	R	R/I
Het publiceren van de Handvesten en deze aan belang-hebbenden meedelen	A	C	C	R	R/I
De betrokkenen, bij rechtstreekse verzameling, informeren over de verwerkingsactiviteiten op het moment van verzameling (zie de te verstrekken informatie in artikel 13 van de GDPR).	A	C			
De betrokkenen, in geval van indirecte inzameling, zo spoedig mogelijk en uiterlijk bij de eerste mededeling, maar altijd binnen een maand, informeren (zie de mee te delen informatie in artikel 14 GDPR)	A	C			

Rapporten (Deliverables)

- "Privacyverklaring" of het "Handvest van de bescherming van persoonsgegevens", ondermeer gepubliceerd op de website
- Lijst van verzamel- en communicatiekanalen met de betrokkenen
- Lijst van de verwerkingen per betrokkene
- Interne informatie (voor werknemers en interne medewerkers)

C4. Bewustwording en opleiding

Art. 24

Regelmatige organisatie van bewustmakings- en opleidingsactiviteiten voor de medewerkers (intern en extern) met betrekking tot het inzicht in de verwerkingen, de risico's, de gegevensbeschermingsmaatregelen en de rechten van de betrokkenen.

Matrix voor goede praktijken en verantwoordelijkheid:

Rollen / Praktijken	VV	[D]PO	GDPR-contactpersoon	CISO	IT/PMO	HR	GV Afdeling
Het bepalen van de categorieën van doelgroep en per categorie van de de behoeften aan bewust-making of opleiding op dit gebied	A	R/S	C	C	C	R/C	R/C
Voorbereiding van de bewustmaking en opleiding	A	R/S	C	R	C	R	C
Het organiserne van opleidingen per categorie van doelgroep	A	R/S	R	I	(R)	I	R
Bijhouden van bewijsstukken van bewustmaking en opleiding, en een lijst van degenen die daaraan hebben deelgenomen	A	R/S	R		C	C	C
De bijwerking of herhaling van bewustmaking/opleiding en het bijhouden van bewijzen	A	R/S	C	R	C	R	C
Het organiserne van regelmatige tests of quizzen om de kennis te toetsen	A	R/S	C	C		C	I

Rapporten (Deliverables)

- Matrix voor bewustmakings- en opleidingsbehoeften - per doelgroep
- Bewustmakingsmateriaal (GDPR en veiligheid)
- Opleidingsmateriaal (GDPR en veiligheid)
- Bewijzen van opleiding
- Bewijs van bewustmaking van de doelgroepen
- Bewijs van bijscholing en permanente opleiding/bewustmaking
- Resultaten van de regelmatige tests

C5. Businesscontinuïteitsbeheer (BCP)

Art. 32

Er worden passende maatregelen getroffen om de continuïteit van de activiteiten met betrekking tot persoonsgegevens voor de betrokkenen te waarborgen.

Matrix voor goede praktijken en verantwoordelijkheid:

Rollen / Praktijken	VV	[D]PO	GDPR-contactpersoon	CISO	Business Continuity Manager[40]	GV Afdeling
Vaststellen van de behoefte aan continuïteit bij de verwerking door de GV-afdelingen, ondermeer door door een bedrijfseffectenbeoordeling (BIA - Business Impact Analysis) op te stellen	A	C/I	C	C	R	C
Het evalueren van de continuïteits-risico's en de vaststelling van maximale dienstonderbrekingen (RTO - Recovery Time Objective) en het maximaal verlies aan persoonsgegevens (RPO - Recovery Point Objective)	A	C/I	C	C	R	C
De integratie van de continuïteits- en herstelmaatregelen van de GV-afdeling in het bedrijfscontinuïteitsplan (BCP)	A	C/I	C	C	R	C
De opleiding in bedrijfscontinuïteits-planning	A	I	I	C	R	I
Het inoefenen en testen van het bedrijfscontinuïteitsplan	A	C/I	C	R	R	R
De evaluatie en verbetering van het bedrijfscontinuïteitsplan	A	C/I	C	C	R	C
Het beheer van de Back-up middelen	A	C/I	C	C	R	C
In geval van herstel, een post-recovery onderzoek uitvoeren.	A	C/I	C	C	R	C

Rapporten (Deliverables)

- Bedrijfseffectbeoordeling - BIA
- Continuïteitsrisicobeoordeling, inclusief RTO en RPO
- Bedrijfscontinuïteitsplan (BCP)
- Opleidingsplan inzake het BCP
- Notulen van de test van het bedrijfscontinuïteitsplan
- Maatregelen ter verbetering van het bedrijfscontinuïteitsplan
- Back-up plan
- Verslag van het onderzoek na het herstel

[40] De functie van Bedrijfscontinuïteitsmanager wordt vaak gecombineerd met die van CISO.

C6. Beheer en kennisgeving van inbreuken in verband met persoonsgegevens

Art. 33-34

De maatregelen, die noodzakelijk zijn om een efficiënt beheer van inbreuken in verband met persoonsgegevens, worden uitgevoerd.

Matrix voor goede praktijken en verantwoordelijkheid:

Rollen / Praktijken	VV	[D]PO	GDPR-contactpersoon	Incident Manager[41]	RSSI	GV Afdeling
Het vaststellen en implementeren van een procedure voor het beheer van inbreuken in verband met persoonsgegevens vaststellen en uitvoeren (vanaf de opsporing, de melding, de vaststelling van de inbreuk, tot het nemen van maatregelen om de gevolgen en de impact ervan te beperken, de eventuele kennisgeving aan de gegevensbeschermingsautoriteit en/of de betrokkenen, de analyse van de oorzaken om nieuwe inbreuken te voorkomen en de evaluatie van het beheer)	A	R/S	C	C/I	C/I	C/I
Het aanmaken, uitvoeren (en bijhouden) van een intern register van inbreuken	A	R/S	C	R	R/C	C
Uitwerken van mechanismen voor het opsporen van incidenten door middel van monitoring en rapportage [42]	A			R		
In geval van een vermoedelijke inbreuk: • Het verzamelen van relevante informatie • De analyse om na te gaan of er sprake is van een inbreuk en deze te kwalificeren (betrokkenheid van persoonsgegevens, ernst, omvang) • Het documenteren van het incident • Het bepalen van antwoorden (maatregelen)	A	C	C	R	C	C
In geval van een inbreuk: • Het te bepalen of de GBA en eventueel de betrokkenen in kennis moeten worden gesteld • Indien nodig de kennisgeving aan de GBA • Indien nodig de kennisgeving aan de betrokkenen	A	R C C	C	C R R	C	I (R) R
Ervoor zorgen dat de inbreuken door de VV binnen de vereiste kennisgevingstermijnen worden gemeld	A	R				
Het trekken van lessen uit en het geven van feedback over incidenten en inbreuken met het oog op voortdurende verbetering	A	R/C	C	R	R	C

[41] De rol van incidentmanager kan worden toegewezen aan de CISO, een IT-deskundige of een specifieke functie, afhankelijk van de omvang en structuur van de organisatie.
[42] De identificatie moet worden geïntegreerd in de incidentbeheersprocessen van de organisatie.

Rapporten (Deliverables)

- Intern register van inbreuken
- Methode voor het beoordelen van het risico voor betrokkenen in geval van een inbreuk in verband met persoonsgegevens
- Modelvragenlijst om alle nodige informatie te verkrijgen in geval van een (vermoedelijke) inbreuk in verband met gegevens
- Modelverslag over het beheer van het incident (de inbreuk), met inbegrip van de maatregelen die zijn genomen om de gevolgen van het incident (en verdere voorvallen) te beperken.
- Kennisgeving aan de GBA en/of de betrokkene

C7. Bescherming en beveiliging van persoonsgegevens

Art. 32

Er zullen passende organisatorische en technische maatregelen worden getroffen om de persoonsgegevens van de betrokkenen op passende wijze te beschermen.

Matrix voor goede praktijken en verantwoordelijkheid:

Rollen / Praktijken	VV	[D]PO	GDPR-contactpersoon	CISO	IT/PMO	GV Afdeling
Het integreren van de maatregelen ter bescherming van persoonsgegevens integreren in het beheerssysteem voor informatiebeveiliging (ISMS - Information security-management system)	A	C	C	R	C	C
Het vaststellen, per gegevensverwerking, van de passende organisatorische en technische maatregelen[43]	A	C	C	R	C	C
Het treffen van de beschermings- en beveiligings-maatregelen, met inbegrip van maatregelen ter voorkoming van gegevensverlies en bescherming tegen cybercriminaliteit	A	C	C	R	C	I
De vaststelling van beveiligingsprocedures	A	C	C	R	C	C
De communicatie over en bewustmaking van beschermings- en veiligheidsmaatregelen	A	C/R	R	R	I	I
Het invoeren van traceerbaarheid van toegang/wijziging/andere verwerkingen van de GV-afdelingen	A	C	C	R	R	I
Het toezicht houden op de uitvoering van beschermings- en veiligheidsmaatregelen	A	R	R	R	C	C
De evaluatie van beschermings- en veiligheids-maatregelen	A	C/I	C	R	C	C

Rapporten (Deliverables)

- Beheerssysteem voor informatiebeveiliging (ISMS - Information securitymanagement system)
- Organisatorische en technische maatregelen per verwerking door de GV-afdeling, bv. datalocatie, datatransmissie, enz.
- Mededeling van de maatregelen ter bescherming en beveiliging van persoonsgegevens
- Analyse van de tracking van de activiteiten.
- Notulen van de evaluatie van de maatregelen voor de bescherming en beveiliging van persoonsgegevens

[43] Deze dienen vastgelegd te worden met inachtneming van de aard van de gegevens, de risico's voor de rechten en vrijheden, de uitvoeringskosten, de stand van de techniek, de context en de verwerkingsdoeleinden - artikel 32 van de GDPR.

D. Toezicht en opvolging

Mechanismen voor toezicht, follow-up, evaluatie en controle van het systeem dat is opgezet om aan de eisen van de RGPD en de terzake vastgestelde richtsnoeren te voldoen.

Het toezicht moet ervoor zorgen dat het systeem werkt zoals het bedoeld is en zal nagaan of het risicobeheer in de loop van de tijd doeltreffend is.

D1. Toezicht op en herziening van de regeling (door de DPO)

Art. 39.1

De DPO houdt voortdurend toezicht op de naleving van de GDPR binnen de organisatie. Hij of zij organiseert regelmatige herzieningen om de compliance op lange termijn te waarborgen.

Matrix voor goede praktijken en verantwoordelijkheid:

Rollen / Praktijken	VV	[D]PO	GDPR-contactpersoon	CISO	IT/PMO/ GV Alinfdeg	Interne controle[44]	Risico Manager[45]	Compliance Manager[46]	Interne audit
De regelmatige en geplande herziening van de conceptuele doeltreffend-heid[47] van de implementatie van de praktijken ter naleving van de GDPR	A	R	R	C	C	C	C	C	I
De regelmatige en gepland herziening van de doeltreffendheid van de praktijken (*operationele* doeltreffendheid[48]) voor de naleving van de RGPD op regelmatige en geplande basis beoordelen (1e verde-digingslinie - operationeel)[49]	A	R	R	C	C	-	-	-	I
De regelmatige en geplande herziening van de ondersteunende activiteiten voor de uitvoering van de	A	R	R	C	-	C	C	C	I

[44] Zie de definitie van de rol van interne controle in afdeling 3 - Taken en verantwoordelijkheden
[45] Zie de omschrijving van de rol van de risicomanager op in afdeling 3 - Rollen en verantwoordelijkheden.
[46] Zie de definitie van de rol van de nalevingsfunctionaris in Deel 3 - Rollen en verantwoordelijkheden.
[47] *Conceptuele toereikendheid houdt in dat* ervoor wordt gezorgd dat de praktijken zodanig zijn opgezet dat zij voldoen aan de vereisten van de GDPR.
[48] *Operationele toereikendheid* houdt in dat ervoor wordt gezorgd dat de praktijken worden uitgevoerd op een manier die in overeenstemming is met de vereisten van de GDPR, en dat de controles zodanig functioneren dat risicobeheersing mogelijk is.
[49] Zie figuur 1 in hoofdstuk 4 - 3 Verdedigingslinies van het controlemodel

Rollen / Praktijken	VV	[D]PO	GDPR-contactpersoon	CISO	IT/PMO/ GV Alinfdeg	Interne controle[44]	Risico Manager[45]	Compliance Manager[46]	Interne audit
RGPD (2e verdedidings-linie)[50]									
De vaststelling van actie- en verbeteringsplannen	A	R	C	C/I	C/I	C/I	C/I	C/I	I
De rapportering van de bevindingen van de herzieningen rapporteren aan de VV	A/I	R	C	I	-	I	I	I	I

Rapporten (Deliverables)

- Evaluatiedocumenten m.b.t. de conceptuele en operationele doeltreffendheid
- Actie- en verbeteringsplannen voor GDPR-praktijken
- Samenvattend verslag van de evaluaties voor de Verwerkingsverantwoordelijke

[50] Zie figuur 1 in hoofdstuk 4 - 3 verdedigingslinies van het controlemodel

D2. Herziening van de GDPR naleving (door de andere actoren van de beheerslijnen dan de DPO)

Art. 24

Er moeten passende controleactiviteiten door de verschillende actoren in de tweede verdedigingslinie worden gepland om de naleving van de GDPR te waarborgen.

De controle verschaft redelijke zekerheid over de naleving van de GDPR door het beoordelen controleactiviteiten van de van de 1e en 2e verdedigingslinie. Deze 3e controlelijn is bedoeld om de risico's nog meer te beperken.

Matrix voor goede praktijken en verantwoordelijkheid:

Rollen / Praktijken	VV	Auditcomité	[D]PO /GDPR-contactpersoon	CISO	IT/PMO/ GV Afdeling	interne controle	Risico Manager	Compliance Manager	Interne audit
De regelmatige en geplande herziening van de GPDR-controle-maatregelen (1e verdedigings-linies - operationeel)	A		C	C	C	R		I	I
De integratie van de risico-beoordeling van de GDPR in het risicobeheer van de organisatie	A		C	C	C	C	R	I	I
Het bepalen van het plan voor verbetering van de controle-maatregelen	A		C	C/I	C/I	R	I	I	I
De follow-up van actieplannen (door interne controle)	A		C/I	C/I	C/I	R	C/I	C/I	I
De ontwikkeling van het auditprogramma van de GDPR naleving, met inbegrip van de verwerkers	C	A	C	C	C	C	C	C	R
Het uitvoeren van de compliance audit van de GDPR	C	A	C	C	C	C	C	C	R
Het bepalen van het actieplan	I	A/I	R/I	R/I	R/I	R/I	R/I	R/I	S
De follow-up van het actieplan	I	A/I	C/I	C/I	C/I	C/I	C/I	C/I	R
Het opstellen van het auditverslag en de presentatie van de bevindingen	I	A/I	I	I	I	I	I	I	R
De follow-up van de actieplannen (na de audit)	I	A/I	C/I	C/I	C/I	C/I	C/I	C/I	R

Rapporten (Deliverables)

- Herziening van de controlemaatregelen (door Interne Controle)
- Beheer van de risico's in verband met de bescherming van persoonsgegevens
- Plan om de controlemaatregelen te verbeteren
- Controleverslag

- Actieplan (na de audit)
- Monitoringverslag over de uitvoering van de actieplannen

D3. Controle door de Gegevensbeschermingsautoriteit

Er moeten passende maatregelen worden genomen om te anticiperen op de controle en inspecties door de GBA en deze mogelijk te maken. Dit omvat het opstellen van documentatie en het aantonen van de naleving van de GDPR (documentenbeheer) overeenkomstig het *verantwoordingsbeginsel*[51]

Matrix voor goede praktijken en verantwoordelijkheid:

Rollen / Praktijken	Verwerkingsverantwoordelijke (VV)	[D]PO	GDPR-contactpersoon	CISO	IT/PMO GV Afdeling	Interne Controle / Risicomanager / Compliance Manager	Audit Interne
Het in kaart brengen van potentiële controles en inspecties door de autoriteiten	A	R					
Het opzetten van een archief/documentenbeheer van registers, procedures, contracten, kennisgevingen en andere documenten om te documenteren dat de VV de beginselen en verplichtingen van de GDPR naleeft	A	R/C	C/I	R/C/I	R/C/I	C/I	I
Het vastleggen de procedure in geval van een controle ter plaatse door de GBA	A	R	C/I	C/I	C/I	C/I	I
Het vaststellen van de procedure om te reageren op een schriftelijk verzoek van de GBA	A	R					
Het aanwijzen van contactpunten en locatiemanagers	A	R	C/I	C/I	C/I	C/I	I
Het vastleggen van het gedrag van de medewerkers	A	R	C/I	C/I	C/I	C/I	I
Het verduidelijken van de rol van de DPO, de locatiemanagers en de belangrijkste contactpersonen	A	R	C/I	C/I	C/I	C/I	I
De opleiding van diegenen om een inspectie door de GBA te begeleiding vanaf de aankomst	A	R	I	I	I	I	I

[51] Artikel 5, lid 2, van de GDPR

Rapporten (Deliverables)

- Lijst van de controles (de zaken die de GBA zou kunnen controleren) en mogelijke inspecties
- Directory / Documentenbeheer van documenten en registers
- Procedure voor de inspectie ter plaatse
- Procedure om het reageren op een schriftelijk verzoek van de GBA
- Lijst van contactpunten en locatiemanagers
- Gedragscode voor werknemers
- Rol van de DPO, locatiemanagers en bevoorrechte gesprekspartners
- Opleidingsmateriaal m.b.t. het toezicht door de GBA

Bijlage 1 - Woordenlijst

De onderstaande tabel geeft een overzicht van de gebruikte afkortingen met hun betekenis in het Nederlands en het Engels.

Afkorting	Nederlandstalige definitie	Engelse definitie
AVG	Algemene Verordening Gegevensbescherming	General Data Protection Regulation (GDPR)
BCP	Bedrijfscontinuïteitsplan	Business Continuity Plan
BIA	Business Impact analyse	Business Impact Analysis
CISO	Hoofd informatiebeveiliging / beveiligingsadviseur / beveilingsconsulent	Chief Information Security Officer
DPbD	Gegevensbescherming door ontwerp	Data Protection by Design
DPbDf	Gegevensbescherming door standaardinstellingen	Data Protection by default
DPIA	Gegevensbeschermingseffect-beoordeling	Data Protection Impact Analysis
DPO	Functionaris voor gegevensbescherming (FvG)	Data Protection Officer
(D)TIA	(Gegevens)overdrachtseffect-beoordeling	(Data) Transfer Impact Assessment
EDPB	Europees Comité voor gegevensbescherming	European Data Protection Board (EDPB)
GBA	Gegevensbeschermingsautoriteit	Data Protection Authority (DPA) / Supervisory authority
HR	Human Resources afdeling (Personeelsdienst)	Human Resources department (HR)
IA	Interne audit	Internal Audit
IC	Interne controle	Internal Control
ISSP	Informatiebeveiligingsbeleid	Information Security Systems Policy
IT	IT-afdeling	Information Technology department
EER	Europese Economische Ruimte	European Economic Area (EEA)
PMO	Project Management Office / Projectbureau	Project Management Office
PO	Privacy Officer / Privacy Functionaris	Privacy Officer

Afkorting	Nederlandstalige definitie	Engelse definitie
RACI	Verantwoordelijkhedenmatrix: Verantwoordelijk (R), Eindverantwoordelijk (A), Geraadpleegd (C), Geïnformeerd (I)	Responsibility matrix: Responsible, Accountable, Consulted, Informed
RPO	Herstelpuntdoelstelling – Hoeveel data kan de organisatie missen? Het laatste herstelpunt.	Recovery Point Objective
RTO	Hersteltijddoelstelling – Hoe lang mag het duren eer de organisatie up-and-running is na een incident?	Recovery Time Objective
SCC	Modelcontractbepalingen	Standard Contractual Clauses
ISMS	Managementsysteem voor informatiebeveiliging	Information Security Management System (ISMS)
VV	Verwerkingsverantwoordelijke	Controller
VW	Verwerker	Processor