Borgingsproduct AVG versie 3.0
Toetsingskader

Hfd	Titel	type	Uitleg	Beantwoording	Toelichting antwoord	invul	Domein	Proces	AVG	BP v2	PCF Norea
1.	Beleid	hfd									
1.1	Beleid vaststellen	par	Beleidsstukken en uitwerkingen daarvan worden gestructureerd vastgesteld en bekendgemaakt.						24 lid 2		
1.1.1	De organisatie heeft beleid ten aanzien van het vaststellen, publiceren en archiveren van interne beleidsstukken en uitwerkingen daarvan, zoals procedures en standaarden.	sub	De organisatie behoort de kaders te stellen waarbinnen beleid wordt gemaakt. Stel daarbij regels zodat beleidsdocumenten herkenbaar zijn, en dat er adequaat documentmanagement plaatsvindt. Daardoor kan er geen onduidelijkheid bestaan over de status van een document.	Ja		binair				1.1.7	Leeg
1.1.2	Beleidsstukken die van toepassing zijn op de gehele organisatie hebben een centrale vindplaats.	sub	Een centrale vindplaats zorgt ervoor dat medewerkers weten waar ze authentieke versies van beleidsstukken kunnen vinden.	Ja		binair				Leeg	Leeg
1.2	Privacybeleid	par	Er is privacybeleid vastgesteld voor de gehele organisatie.						24 lid 2		
1.2.1	Het privacybeleid beschrijft hoe de organisatie uitvoering geeft aan de privacybeginselen die in art. 5 lid 1 AVG zijn vastgelegd.	sub		Ja		binair				1.1.1	PP003; PP004; DMI02; ULI02
1.2.2	Het privacybeleid beschrijft hoe de organisatie uitvoering geeft aan de verplichtingen die op de organisatie rusten op grond van privacywetgeving en materiewetgeving bij de verwerking van persoonsgegevens.	sub		Ja		binair	X			Leeg	PP003
1.2.3	Het privacybeleid beschrijft de rollen, taken en verantwoordelijkheden van de functionarissen die bij de uitvoering van het beleid zijn betrokken.	sub	De organisatie kan ervoor kiezen om een gedetailleerde uitwerking hiervan vast te leggen in andere beleidsstukken.	Ja		binair	X			1.2.2	PP002
1.2.4	Het privacybeleid is formeel vastgesteld door het verantwoordelijke bestuursorgaan.	sub		Ja		binair				1.1.3	PP001
1.2.5	Het privacybeleid is bekendgemaakt binnen de gehele organisatie.	sub	Het is aanbevelenswaardig om bij wijzigingen in het beleid hier eveneens een communicatie aan te wijden.	Ja		binair				1.1.4	PP001
1.2.6	Het privacybeleid wordt periodiek, maar ten minste eenmaal per 36 maanden, herzien.	sub	Bij een herziening is het niet altijd noodzakelijk om wijzigingen door te voeren. Het is wel van belang dat de organisatie periodiek heroverweegt of het beleid nog aansluit bij interne en externe ontwikkelingen.	Ja		binair	X			Leeg	PP001
1.2.7	Beleidsdocumenten over andere onderwerpen zijn in lijn met het privacybeleid.	sub	Privacy kent overlap of aanknopingspunten met ander beleid in de organisatie. Denk bijvoorbeeld aan het informatiebeveiligingsbeleid, archiefbeleid en personeelsbeleid. Dit beleid moet op elkaar aansluiten en waar nodig naar elkaar verwijzen.	In enkele gevallen (≤ 35%)		schaal	X			1.1.6	Leeg
1.2.8	De organisatie heeft geïnventariseerd voor welke domeinen het noodzakelijk is om over domeinspecifieke uitwerkingen van het privacybeleid te beschikken om correcte omgang met persoonsgegevens binnen het desbetreffende domein te verzekeren.	sub		In geen enkel geval (≤ 5%)		schaal	X			1.1.5	Leeg

1.2.9	De organisatie heeft domeinspecifieke uitwerkingen van het privacybeleid vastgesteld voor de domeinen waarvoor dit noodzakelijk is.	sub		In geen enkel geval (≤ 5%)	schaal	X			1.1.5	Leeg
1.3	Verantwoordelijkheden	par	Verantwoordelijkheden voor het realiseren van de doelstellingen van het privacybeleid zijn benoemd, belegd en vastgesteld.					38		
1.3.1	In beleid is vastgelegd dat het management verantwoordelijk is voor het realiseren van de doelstellingen van het privacybeleid van de organisatie.	sub	De lijnmanager kan voor wat betreft ondersteuning een beroep doen op een privacy officer, maar blijft zelf eindverantwoordelijk.	Ja	binair				1.2.1	PP002
1.3.2	In beleid is vastgelegd dat het management advies inwint bij een privacy specialist alvorens aangevangen wordt met een nieuwe of verdere verwerking van persoonsgegevens.	sub		Nee	binair				Leeg	TPD01
1.3.3	Het lijnmanagement wint in de praktijk daadwerkelijk advies in van een privacy specialist alvorens aangevangen wordt met een nieuwe of verdere verwerking van persoonsgegevens.	sub		In enkele gevallen (≤ 35%)	schaal				Leeg	TPD01
1.3.4	In beleid is vastgelegd dat het management verantwoordelijk is om keuzes te maken op het gebied van privacyrisico's, zoals het treffen van mitigerende maatregelen en het accepteren van restrisico's.	sub	Aanbevolen wordt om een RASCI matrix te hanteren, en dit in het privacybeleid vast te leggen.	Ja	binair				1.2.5	RMA04
1.3.5	In beleid is vastgelegd dat het management bij het uitvoeren van privacyrisicomanagement wordt ondersteund door een deskundige op dat gebied.	sub		In enkele gevallen (≤ 35%)	schaal				Leeg	RRE04
1.3.6	Het management beschikt over voldoende (financiële) middelen om het privacybeleid adequaat uit te voeren.	sub		In alle gevallen (≥ 95%)	schaal	X			Leeg	SCO04
2.	Processen	hfd								
2.1	Werkprocessen	par	De organisatie heeft de werkprocessen waarin persoonsgegevens worden verwerkt in beeld en beschreven.					24 lid 1		
2.1.1	Werkprocessen waarbinnen persoonsgegevens worden verwerkt zijn eenduidig beschreven en vastgesteld.	sub	Het gaat hier om de processen van de organisatie die een bepaalde nuttige uitkomst hebben voor klanten van de organisatie of de organisatie zelf. Zoals een proces van vergunningverlening, of een proces van indiensttreding. Dergelijke processen kunnen meerdere verwerkingen van gegevens omvatten. Het inzichtelijk hebben van werkprocessen en de IT systemen die daar ondersteunend aan zijn vormt een belangrijk aanknopingspunt om gegevensverwerkingen te identificeren en te beheersen. Eén proces kan meerdere gegevensverwerkingen omvatten.	In enkele gevallen (≤ 35%)	schaal	X	X		2.1.1; 2.1.2	PDI01
2.1.2	Alle werkprocessen hebben een proceseigenaar (de manager die verantwoordelijk is voor het proces).	sub		Ja	binair	X	X		Leeg	PDI01
2.1.3	De organisatie heeft een totaaloverzicht van werkprocessen waarbinnen persoonsgegevens worden verwerkt.	sub	Zowel processen die noodzakelijk zijn voor de dienstverlening van de organisatie als ondersteunende processen (bijv. HR processen) behoren inzichtelijk te zijn.	Ja	binair	X	X		2.1.3	PDI01

2.1.4	De organisatie heeft inzichtelijk welke werkprocessen geheel of gedeeltelijk handmatig worden uitgevoerd.	sub	Denk hierbij bijvoorbeeld aan processen waarbij handmatige invoer van data plaatsvindt, zoals meldingen die telefonisch worden aangenomen door het KCC.	In enkele gevallen (≤ 35%)	schaal	X	X		Leeg	PDI01
2.1.5	Geheel of gedeeltelijk handmatig uitgevoerde processen worden ondersteund door werkinstructies, waarin is vastgelegd wat wordt verwacht van de medewerker met het oog op de privacy van de betrokkene.	sub		In geen enkel geval (≤ 5%)	schaal	X	X		2.2.1	STR01; LOG01
2.1.6	Werkinstructies zijn eenvoudig toegankelijk voor medewerkers.	sub		In alle gevallen (≥ 95%)	schaal	X	X		2.2.2	Leeg
2.1.7	De organisatie evalueert periodiek of de beschrijvingen van werkprocessen aansluiten bij de praktijk.	sub	Wanneer de procesbeschrijvingen niet actueel zijn, kan de organisatie niet aantonen dat de verwerkingen van persoonsgegevens in overeenstemming met de AVG worden uitgevoerd (art. 24 lid 1 AVG).	In enkele gevallen (≤ 35%)	schaal	X	X		2.1.4	PDI01
2.2	Verwerkingsregister	par	De organisatie houdt een verwerkingsregister bij dat voldoet aan de bij wet gestelde eisen en houdt deze continu actueel.					30		
2.2.1	Alle bij wet voorgeschreven onderdelen zijn in het verwerkingsregister aanwezig (art. 30 lid 1 en lid 2 AVG).	sub	Het is aanbevelenswaardig om de verwerkingen op afdelingsniveau inzichtelijk te maken. Naast de wettelijk voorgeschreven velden is het aanbevelenswaardig om het verwerkingsregister als tool te gebruiken om additionele registraties bij te houden. Zoals of een DPIA moet worden uitgevoerd, en zo ja, of en wanneer deze is uitgevoerd.	Ja	binair				2.3.1	PDI02; PDI03; PDI04
2.2.2	In het verwerkingsregister is voor iedere verwerking vastgelegd of de organisatie verwerkingsverantwoordelijke, verwerker of gezamenlijk verwerkingsverantwoordelijke is.	sub		Ja	binair	X	X		2.3.1	RRE01
2.2.3	De organisatie heeft alle verwerkingen van persoonsgegevens correct vastgelegd in het register en het register is up-to-date.	sub	Als er nog velden zijn met ontbrekende data, dan is de verwerking niet correct vastgelegd in het register.	In enkele gevallen (≤ 35%)	schaal	X	X		2.3.8	PDI04; PIA05
2.2.4	Het register kan desgevraagd aan de AP worden overhandigd.	sub	Het register is in een vorm opgesteld die het mogelijk maakt het register gemakkelijk te delen met de autoriteiten.	Ja	binair				2.3.3	Leeg
2.2.5	De organisatie heeft voor iedere verwerking vastgesteld dat deze plaatsvindt in overeenstemming met de privacybeginselen. Bij wijziging van een verwerking wordt deze beoordeling opnieuw uitgevoerd.	sub	De privacybeginselen zijn vastgelegd in art. 5 lid 1 AVG. Samengevat gaat het om rechtmatigheid, behoorlijkheid, transparantie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking en beveiliging.	In enkele gevallen (≤ 35%)	schaal	X	X		2.3.7	PP005; PDI03; LRC01; CFR03; DMI01; URE03; ACD01; ACD02
2.2.6	Er is vastgelegd welke functionaris eindverantwoordelijk is voor het proces dat de volledigheid en accuraatheid van het verwerkingsregister waarborgt.	sub	Aanbevolen wordt om bijv. een PO verantwoordelijk te maken voor deze taak, en de taken van de FG te beperken tot controles op het register en het proces om het register actueel te houden.	Ja	binair				2.3.4	RRE05
2.2.7	Voor iedere verwerking is een eigenaar vastgesteld.	sub	In de regel zal de eigenaar van een operationeel proces eveneens eigenaar zijn van de individuele verwerkingen die binnen dat proces plaatsvinden.	In alle gevallen (≥ 95%)	schaal	X	X		2.3.5	RRE05
2.2.8	In een procedure is vastgelegd waar nieuwe en gewijzigde verwerkingen moeten worden gemeld teneinde deze op te nemen in het verwerkingsregister.	sub		Nee	binair				2.3.6	Leeg

2.2.9	In een procedure is vastgesteld met welke interval een beoordeling wordt uitgevoerd of het verwerkingsregister nog volledig en actueel is en welke functionaris hiervoor verantwoordelijk is.	sub		Nee	binair				Leeg	Leeg
2.2.10	De organisatie beoordeelt periodiek of het verwerkingsregister actueel en volledig is.	sub		In de meeste gevallen (< 95%)	schaal				2.3.10	Leeg
2.3	Pre-DPIA's	par	De organisatie identificeert systematisch of verwerkingen een hoog risico in kunnen houden voor de rechten en vrijheden van betrokkenen					35		
2.3.1	De organisatie heeft een procedure om voor alle nieuwe en gewijzigde verwerkingen te bepalen of deze mogelijkerwijs een hoog risico inhouden voor de rechten en vrijheden van betrokkenen.	sub		Ja	binair				2.4.1; 2.4.3	RMA03; LRC01; PBD01
2.3.2	De organisatie heeft voor alle verwerkingen bepaald of deze een hoog risico kunnen opleveren.	sub	Aanbevolen wordt om dit als additioneel veld op te nemen in het verwerkingsregister.	In geen enkel geval (≤ 5%)	schaal	X	X		2.4.4	PIA01
2.3.3	De analyse die ten grondslag ligt aan het besluit of een verwerking al dan niet een hoog risico kan opleveren is gedocumenteerd.	sub		In geen enkel geval (≤ 5%)	schaal	X	X		2.4.4	RMA03
2.4	DPIA's	par	Indien een verwerking is geïdentificeerd die een hoog risico kan opleveren, wordt een DPIA uitgevoerd die aan de eisen van de AVG voldoet. De organisatie beheert de uitkomsten van DPIA's systematisch.					35		
2.4.1	Er is een procedure vastgesteld voor het uitvoeren van DPIA's op nieuwe en sterk gewijzigde verwerkingen die mogelijkerwijs een hoog privacyrisico inhouden.	sub		Ja	binair				2.4.2	RMA01
2.4.2	Het rapport voor een DPIA is gestandaardiseerd en voldoet aan de wettelijke vereisten.	sub		Ja	binair				2.4.8	PIA02; PIA04
2.4.3	De organisatie heeft voor alle geïdentificeerde hoog-risico verwerkingen een DPIA uitgevoerd.	sub		In geen enkel geval (≤ 5%)	schaal	X	X		Leeg	PIA01
2.4.4	Er is een procedure vastgesteld voor het opvolgen (behandelen of accepteren) van risico's die in een DPIA zijn geïdentificeerd.	sub		Ja	binair				2.4.14; 2.4.15; 7.2.2	RMA05; PIA06
2.4.5	De organisatie beheert in DPIA's geïdentificeerde risico's en te implementeren maatregelen op een centrale plaats.	sub		In geen enkel geval (≤ 5%)	schaal	X	X		Leeg	PIA06
2.4.6	De procedure voor DPIA's schrijft voor dat de FG bij het uitvoeren van een DPIA ten minste wordt geconsulteerd en dat het advies van de FG schriftelijk wordt vastgelegd.	sub		Ja	binair				2.4.6; 3.1.8	RRE04; PIA04
2.4.7	Voor alle uitgevoerde DPIA's is een schriftelijk advies van de FG vastgelegd.	sub		In geen enkel geval (≤ 5%)	schaal	X	X		Leeg	Leeg
2.4.8	De procedure voor DPIA's schrijft voor dat wanneer wordt afgeweken van het advies van de FG dit schriftelijk wordt vastgelegd, en stelt eveneens vast welke functionaris beslissingsbevoegd is ten aanzien van dit besluit.	sub		Nee	binair				2.4.7; 2.4.9	RRE05
2.4.9	De organisatie controleert periodiek of naar aanleiding van een DPIA te implementeren maatregelen daadwerkelijk worden geïmplementeerd en het beoogd effect bereiken.	sub		In geen enkel geval (≤ 5%)	schaal	X	X		2.4.14	PIA06

2.4.10	De organisatie controleert periodiek of er een actuele DPIA beschikbaar is voor alle verwerkingen met een hoog privacyrisico.	sub		In geen enkel geval (≤ 5%)	schaal				2.4.17; 7.2.1	Leeg
2.5	Bewaar- en vernietigingsbeleid	par	Persoonsgegevens worden tijdig verwijderd of geanonimiseerd.					5 lid 1 sub c		
2.5.1	Er is beleid vastgesteld voor het verwijderen en anonimiseren van gegevens ('bewaarbeleid').	sub	Het borgingsproduct hanteert verwijderen als synoniem voor vernietigen. Wanneer de organisatie hiervan afwijkt, dient dit in de systematiek die in het beleid wordt beschreven voor vernietigen van persoonsgegevens terug te komen.	Ja	binair	X	X		2.5.4	DRE01; DDA01
2.5.2	Waar noodzakelijk zijn specifieke procedures vastgesteld voor het verwijderen van gegevens, waarin is vastgesteld wat de toepasselijke bewaartermijn is en op welke wijze verwijdering plaats dient te vinden.	sub	De procedures zijn de toepassing van het beleid in een specifiek geval. Procedures hebben betrekking op een of meer concrete verwerkingen en stellen voor die verwerking eenduidig vast wat de bewaartermijn is of hoe deze kan worden bepaald.	In alle gevallen (≥ 95%)	schaal	X	X		2.5.5	DRE01; DRE02; DDA01; DDA02
2.5.3	Het bewaarbeleid is ook van toepassing op logging en back-ups, voor zover deze persoonsgegevens bevatten.	sub		In alle gevallen (≥ 95%)	schaal	X	X		2.5.7	DRE01; DDA01; ENC03
2.5.4	Persoonsgegevens worden verwijderd of geanonimiseerd in overeenstemming met de Selectielijst 2020.	sub	De selectielijst is van toepassing op papieren en digitale gegevens. Papieren documenten zijn onderhevig aan de AVG als ze opgenomen zijn (of bestemd zijn om opgenomen te worden in) in een bestand.	In alle gevallen (≥ 95%)	schaal	X	X		2.5.1	DRE02
2.5.5	Indien er geen termijn uit de Selectielijst 2020 van toepassing is worden de persoonsgegevens verwijderd of geanonimiseerd na het verstrijken van de wettelijke bewaartermijn.	sub		In alle gevallen (≥ 95%)	schaal	X	X		2.5.2	DRE02
2.5.6	Indien er ook geen wettelijke bewaartermijn van toepassing is worden de persoonsgegevens verwijderd of geanonimiseerd wanneer ze niet meer nodig zijn voor het doel waarvoor ze verzameld zijn.	sub		In geen enkel geval (≤ 5%)	schaal	X	X		2.5.3	DRE02
2.5.7	Waar mogelijk wordt het verwijderen of anonimiseren van persoonsgegevens geautomatiseerd uitgevoerd.	sub		In ongeveer de helft van de gevallen (≤ 65%)	schaal	X	X		Leeg	DDA01
2.5.8	De organisatie controleert periodiek of applicaties daadwerkelijk verwijderen of anonimiseren conform het bewaarbeleid.	sub	Niet altijd werkt een applicatie naar behoren (bijv. als gevolg van een bug geïntroduceerd bij een update). Daarom is het van belang om te checken of verwijdering plaatsvindt conform de voorschriften.	Ja	binair	X	X		2.5.6	DDA01
3.	Organisatorische inbedding	hfd								
3.1	Privacyteam	par	Er is – naast de FG - ruime kennis en ervaring aanwezig over privacywetgeving.							
3.1.1	Er is voldoende capaciteit van een of meer privacy specialisten beschikbaar om het management te ondersteunen bij het realiseren van de doelstellingen van het privacybeleid.	sub		In de meeste gevallen (< 95%)	schaal	X			3.2.1	RRE04; SCO04
3.1.2	Er is een functionaris verantwoordelijk voor het tijdig inschatten van de gevolgen voor de organisatie van ontwikkelingen op het gebied van privacywetgeving en jurisprudentie.	sub		Ja	binair				2.7.3; 2.7.4	LRC01

3.2	Aanstelling, positie en taken FG	par	De organisatie heeft een FG aangesteld en zodanig gepositioneerd dat deze effectief toezicht kan houden.					37; 38; 39		
3.2.1	De organisatie heeft een FG aangesteld.	sub	Voor gemeenten geldt dat de burgmeester, B&W en de raad allen een FG dienen aan te wijzen.	Ja	binair			Leeg	Leeg
3.2.2	De FG is zodanig gepositioneerd in de organisatie dat hij als onafhankelijk toezichthouder kan functioneren.	sub		Ja	binair			Leeg	Leeg
3.2.3	De FG is op basis van zijn aanstellingsbesluit verantwoordelijk voor het toezien op de naleving van de AVG en het rapporteren daarover aan het bestuursorgaan.	sub		Ja	binair			Leeg	RRE04
3.2.4	De FG heeft op basis van zijn aanstellingsbesluit de bevoegdheid om verwerkingsactiviteiten te controleren.	sub	Dit kan bijvoorbeeld in het functieprofiel of in het aanstellingsbesluit worden vastgelegd.	Ja	binair			3.1.5	Leeg
3.2.5	De FG heeft geen taken of verplichtingen die kunnen leiden tot een belangenconflict bij de uitvoering van zijn taken als FG.	sub		Ja	binair			Leeg	Leeg
3.2.6	De FG ontvangt geen instructies met betrekking tot de uitvoering van zijn taken.	sub		Ja	binair			3.1.1	Leeg
3.2.7	De FG heeft voldoende middelen om zijn deskundigheid op peil te houden	sub		In alle gevallen (≥ 95%)	schaal			3.1.2	SCO01
3.2.8	De FG heeft voldoende tijd en middelen ter beschikking voor het uitoefenen van zijn taken.	sub		In alle gevallen (≥ 95%)	schaal			Leeg	SCO04
3.2.9	De FG voldoet aan de functievereisten uit art. 37 lid 5 AVG.	sub		Ja	binair			Leeg	Leeg
3.2.10	De contactgegevens van de FG zijn makkelijk vindbaar voor betrokkenen.	sub	Zowel interne als externe betrokkenen behoren contract op te kunnen nemen met de FG.	Ja	binair			3.1.6; 4.1.1	Leeg
3.2.11	De FG wordt betrokken bij opleiding en bewustwordingsprogramma's voor personeel op het gebied van privacy.	sub		In alle gevallen (≥ 95%)	schaal	X		Leeg	Leeg
3.3	Informeren OR	par	De Ondernemingsraad (OR) wordt geïnformeerd en betrokken wanneer het gaat om de bescherming van persoonsgegevens van medewerkers.							
3.3.1	De OR wordt om instemming gevraagd als het gaat om een regeling die impact heeft op de bescherming van persoonsgegevens van medewerkers.	sub		In geen enkel geval (≤ 5%)	schaal			3.3.1	Leeg
3.3.2	De OR wordt actief geïnformeerd over privacy en gegevensbescherming voor wat betreft het personeel.	sub		In geen enkel geval (≤ 5%)	schaal			3.3.2	Leeg
3.4	Bewustwording	par	Er zijn voldoende middelen beschikbaar om privacybescherming te bevorderen in kennis, houding en gedrag van medewerkers in de organisatie.							
3.4.1	In contracten met medewerkers en contractanten, die in aanraking komen met persoonsgegevens, wordt ten minste het volgende vastgelegd: - De verantwoordelijkheden met betrekking tot het beschermen en geheimhouden van persoonsgegevens; - De verplichting om persoonsgegevens uitsluitend te verwerken conform de opdrachten en instructies van de verwerkingsverantwoordelijke.	sub		In ongeveer de helft van de gevallen (≤ 65%)	schaal	X		Leeg	Leeg

3.4.2	In een procedure is vastgelegd dat medewerkers en contractanten bij indiensttreding bewust worden gemaakt van hun verantwoordelijkheden met betrekking tot het beschermen en geheimhouden van persoonsgegevens.	sub	Hiervoor kan bijvoorbeeld een verplichte training worden gehanteerd.	Ja	binair	X			3.4.1	SAT01
3.4.3	Alle medewerkers en contractanten hebben aantoonbaar een bewustwordingstraining gevolg die passend is voor hun functie.	sub		In alle gevallen (≥ 95%)	schaal	X			Leeg	SCO03; RRE05; SAT02; SCO02
3.4.4	Er is een programma om medewerkers doorlopend bewust te maken van de risico's en randvoorwaarden bij de omgang met persoonsgegevens (bewustwordingsprogramma).	sub	Het bewustwordingsprogramma kan ook andere namen hebben (bijv. een communicatieplan).	Ja	binair	X			3.4.2	SAT01; SAT02; SAT03
3.4.5	Periodiek wordt het bewustwordingsprogramma getoetst op effectiviteit en waar nodig bijgesteld.	sub		In alle gevallen (≥ 95%)	schaal				Leeg	SAT03
4.	Rechten van de betrokkene	hfd								
4.1	Recht op informatie	par	De organisatie voldoet aan het recht op informatie van de betrokkene.					13; 14		
4.1.1	De organisatie heeft op de website een privacyverklaring gepubliceerd waarin uitleg wordt gegeven over: - De identiteit van de verwerkingsverantwoordelijke; - Contactgegevens van de FG; - Verwerkingsdoeleinden en rechtsgrond; - De betrokken categorieën van persoonsgegevens; - Eventuele ontvangers van persoonsgegevens; - Informatie over doorgifte naar landen buiten de EER; - Bewaartermijn; - Rechten van de betrokkene; - Mogelijkheid om klacht in te dienen bij AP; - Het bestaan van geautomatiseerde besluitvorming.	sub	Aanbevolen wordt om de privacyverklaring te ondersteunen met een verwijzing naar een online gepubliceerd verwerkingsregister. Zorg er bij het publiceren van het verwerkingsregister voor dat: - namen van eigenaren van verwerkingen zijn verwijderd; - er niet op andere wijze gevoelige of aan personen te relateren informatie wordt gepubliceerd; - er geen gevoelige informatie over informatiebeveiliging van de organisatie wordt prijsgegeven. Het publiceren van het register is niet verplicht.	Ja	binair	X	X		4.4.1; 7.3.1; 7.3.2; 7.3.3	PST01; DRE01
4.1.2	De privacyverklaring is in eenvoudige en duidelijke taal opgeschreven.	sub	De informatie moet beknopt, transparant en begrijpelijk zijn. Vermijd jargon zoveel mogelijk.	Ja	binair	X	X		4.4.1	PST02
4.1.3	Wanneer persoonsgegevens bij de betrokkene worden verzameld (bijv. via een applicatie of aanvraagformulier), wordt uitleg gegeven over: - De identiteit van de verwerkingsverantwoordelijke; - Contactgegevens van de FG; - Verwerkingsdoeleinden en rechtsgrond; - Eventuele ontvangers van persoonsgegevens; - Informatie over doorgifte naar landen buiten de EER; - Bewaartermijn; - Rechten van de betrokkene; - Mogelijkheid om klacht in te dienen bij AP; - Het bestaan van geautomatiseerde besluitvorming; - Gevolgen als gegevens niet worden verstrekt.	sub	Deze informatie is complementair aan de algemene privacyverklaring en wordt bijvoorbeeld verstrekt wanneer een burger een online melding doet.	In alle gevallen (≥ 95%)	schaal	X	X		4.3.2; 4.6.1	CFR01; PST01

4.1.4	De organisatie verstrekt aan de betrokkene alle verplichte informatie wanneer de organisatie voornemens is om persoonsgegevens verder te verwerken voor een ander doel dan waarvoor deze zijn verkregen.	sub		In ongeveer de helft van de gevallen (≤ 65%)	schaal	X	X		4.3.2	ULI01
4.1.5	De organisatie evalueert periodiek of betrokkenen tijdig en volledig de verplichte informatie ontvangen en waar nodig wordt dit bijgesteld.	sub		In ongeveer de helft van de gevallen (≤ 65%)	schaal	X	X		4.3.2	Leeg
4.2	Processen rechten van betrokkenen	par	De organisatie heeft processen ingericht om uitvoering te geven aan de rechten van de betrokkene wanneer de betrokkene een verzoek indient.					16; 17; 18; 19; 21		
4.2.1	In de interne processen voor de afhandeling van verzoeken van betrokkenen is ten minste het volgende opgenomen: - Op welke wijze verzoeken kunnen worden ingediend; - Op welke wijze de identiteit van verzoeker wordt vastgesteld; - Wie verantwoordelijk is voor de afhandeling; - De toepasselijke termijnen; - De criteria voor het toewijzen en afwijzen van een verzoek; - Het informeren van ontvangers over een verzoek.	sub		Ja	binair	X			4.1.4; 4.1.9; 4.1.10; 5.1.7	DAR01; DAR03; DAR04; DCR01; DCR03; DCR04; DDR01; DDR02; DDR04; URE02
4.2.2	De organisatie heeft bekendgemaakt op welke wijze en in welke gevallen een betrokkene een verzoek kan indienen tot uitoefening van zijn recht op: - Inzage; - Rectificatie; - Wissing; - Beperking; - Overdraagbaarheid; - Bezwaar.	sub	De rechten van betrokkenen zijn niet in alle gevallen van toepassing. De maatregel schrijft daarom voor dat bekend wordt gemaakt 'in welke gevallen' een bepaald recht van toepassing is.	Ja	binair	X			4.1.3	PST01
4.2.3	Verzoeken kunnen zowel schriftelijk als digitaal worden ingediend.	sub		Ja	binair				4.1.2	Leeg
4.2.4	Betrokkenen krijgen een ontvangstbevestiging van hun verzoek en worden op de hoogte gehouden van de status van de behandeling van het verzoek .	sub		Nee	binair	X			4.1.5; 4.1.8	Leeg
4.2.5	Medewerkers die communicatie van klanten behandelen herkennen een AVG-verzoek en weten naar wie zij deze voor verdere behandeling moeten doorsturen.	sub		In ongeveer de helft van de gevallen (≤ 65%)	schaal	X			4.1.6	Leeg
4.2.6	Een beslissing op een AVG-verzoek - een (gedeeltelijke) toe- of afwijzing - geldt als een besluit in de zin van de Algemene wet bestuursrecht (Awb). De organisatie stuurt een bezwaarclausule onder de beslissing mee.	sub		Ja	binair	X			4.1.7	Leeg
4.2.7	Er is een procesverantwoordelijke voor de afhandeling van verzoeken.	sub		Ja	binair	X			Leeg	Leeg
4.2.8	Verzoeken van betrokkenen tot uitoefening van hun rechten worden binnen de wettelijke termijnen afgehandeld.	sub		In alle gevallen (≥ 95%)	schaal	X			Leeg	URE02; DAR03; DCR01; DDR01

4.2.9	Wanneer een termijn voor het reageren op een verzoek van een betrokkene niet wordt gehaald, wordt dit gesignaleerd, en naderhand geanalyseerd. Op basis van de analyse worden maatregelen getroffen om dit in de toekomst te voorkomen.	sub		Niet van toepassing	schaal				4.1.13	DAR03
4.3	Toestemming	par	De organisatie voldoet aan de wettelijke vereisten wanneer een verwerking is gebaseerd op toestemming.					6 lid 1 sub a; 7; 9 lid 2 sub a		
4.3.1	De organisatie heeft vastgesteld welke verwerkingen op toestemming zijn gebaseerd.	sub	Dit behoort centraal te worden gedocumenteerd in het verwerkingsregister.	Ja	binair	X	X		Leeg	CFR02
4.3.2	Bij verwerkingen die zijn gebaseerd op toestemming wordt toestemming gevraagd in begrijpelijke en duidelijke vorm. De betrokkene stemt door middel van een duidelijke actieve handeling in met het gebruik van zijn gegevens.	sub	Zorg dat de organisatie bij het vragen van toestemming voldoet aan de informatieplicht.	In ongeveer de helft van de gevallen (≤ 65%)	schaal	X	X		4.1.11	CFR02; CFR03
4.3.3	Wanneer een betrokkene toestemming heeft gegeven, wordt dit gedocumenteerd, onder vermelding van datum, tijd en identiteit van de betrokkene.	sub		In de meeste gevallen (< 95%)	schaal	X	X		Leeg	CFR02
4.3.4	De betrokkene krijgt de gelegenheid om te allen tijde zijn toestemming in te trekken en wordt daarbij geïnformeerd over welke gevolgen dat heeft.	sub		In ongeveer de helft van de gevallen (≤ 65%)	schaal	X	X		Leeg	CFR02; CFR03; CFR04
4.4	Geautomatiseerde individuele besluitvorming	par	De organisatie voldoet aan de wettelijke voorwaarden voor geautomatiseerde individuele besluitvorming.					22		
4.4.1	In een register wordt bijgehouden in welke informatiesystemen geautomatiseerde individuele besluitvorming wordt toegepast.	sub		Niet van toepassing	schaal	X	X		4.2.2	Leeg
4.4.2	De organisatie voldoet aan de wettelijke voorwaarden voor geautomatiseerde individuele besluitvorming op basis van persoonsgegevens.	sub		Niet van toepassing	schaal	X	X		4.2.1	DAR01
4.4.3	Voor alle informatiesystemen die geautomatiseerde individuele besluitvorming toepassen is een DPIA uitgevoerd.	sub	In aanvulling op een DPIA is het aanbevelenswaardig (maar niet verplicht) om een ethische afweging te maken omtrent de inzet van een algoritme.	Niet van toepassing	schaal	X	X		4.2.3	PIA01
4.4.4	Voor alle informatiesystemen die geautomatiseerde individuele besluitvorming toepassen is een ethische afweging omtrent de toepassing daarvan gemaakt en vastgelegd.	sub		Niet van toepassing	schaal	X	X		4.2.3	Leeg
4.4.5	De informatiesystemen die geautomatiseerde individuele besluitvorming toepassen, worden regelmatig (minimaal eens per 36 maanden) gecontroleerd en getest op naleving van de privacybeginselen en de wettelijke voorwaarden voor geautomatiseerde individuele besluitvorming.	sub		Niet van toepassing	schaal	X	X		4.2.4	Leeg
4.5	Websites en applicaties	par	De websites en applicaties die toegankelijk zijn voor burgers voldoen aan de privacy- en cookiewetgeving.					13; 14		
4.5.1	De organisatie heeft vastgesteld aan welke eisen websites en applicaties die toegankelijk zijn voor burgers moeten voldoen om privacywetgeving en cookiewetgeving na te leven.	sub	De organisatie maakt hierin bijvoorbeeld keuzes omtrent het gebruik van third party analytics.	Ja	binair	X	X		4.5.3	RMA05

4.5.2	De organisatie heeft vastgesteld dat websites en applicaties die toegankelijk zijn voor burgers voldoen aan privacy- en cookiewetgeving.	sub		In alle gevallen (≥ 95%)	schaal	X	X		Leeg	RMA05
4.5.3	De organisatie evalueert periodiek of websites en applicaties die toegankelijk zijn voor burgers voldoen aan privacy- en cookiewetgeving.	sub		In geen enkel geval (≤ 5%)	schaal				4.5.2	REV01
4.6	Technische ondersteuning	par	Informatiesystemen waarin persoonsgegevens worden verwerkt ondersteunen de uitvoering van de rechten van de betrokkene.					16; 17; 18; 19; 21		
4.6.1	Wanneer een betrokkene een verzoek tot inzage in zijn persoonsgegevens doet, zijn de informatiesystemen waarin persoonsgegevens worden verwerkt technisch in staat om hier gevolg aan te geven. De gegevens worden geëxporteerd naar een algemeen bruikbaar formaat.	sub	Voor de hele paragraaf geldt: het is niet verplicht om specifieke maatregelen te treffen als met bestaande faciliteiten reeds uitvoering aan een verzoek kan worden gegeven.	In alle gevallen (≥ 95%)	schaal	X	X		4.1.14; 4.6.3	DAR01
4.6.2	Wanneer een betrokkene een verzoek tot rectificatie van zijn persoonsgegevens doet, zijn de informatiesystemen waarin persoonsgegevens worden verwerkt technisch in staat om hier gevolg aan te geven.	sub	Let hierbij op dat de back-up strategie van de organisatie voorkomt dat gegevens die na een gehonoreerd verzoek zijn gewijzigd bij een restore niet worden teruggezet in de foutieve vorm.	In alle gevallen (≥ 95%)	schaal	X	X		4.1.14; 4.6.5	DCR01
4.6.3	Wanneer een betrokkene een verzoek tot verwijdering van zijn persoonsgegevens doet, zijn de informatiesystemen waarin persoonsgegevens worden verwerkt technisch in staat om hier gevolg aan te geven.	sub	Let hierbij op dat de back-up strategie van de organisatie voorkomt dat gegevens die na een gehonoreerd verzoek zijn verwijderd bij een restore niet worden teruggezet.	In alle gevallen (≥ 95%)	schaal	X	X		4.1.14; 4.6.5	DDR01
4.6.4	Wanneer een betrokkene een verzoek tot beperking van gegevensverwerking doet, zijn de informatiesystemen waarin persoonsgegevens worden verwerkt technisch in staat om hier gevolg aan te geven.	sub		In alle gevallen (≥ 95%)	schaal	X	X		4.1.14; 4.6.6	URE02
5.	Samenwerking	hfd								
5.1	AVG rollen	par	De organisatie heeft de AVG-rol voor alle betrokken partijen die persoonsgegevens verwerken inzichtelijk en conform de AVG met deze partijen afspraken gemaakt.					26; 28		
5.1.1	De organisatie heeft de AVG-rollen van externe partijen inzichtelijk gemaakt.	sub	De volgende AVG-rollen worden onderscheiden: - Verwerkingsverantwoordelijke; - Verwerker; - Gezamenlijk verwerkingsverantwoordelijke.	In ongeveer de helft van de gevallen (≤ 65%)	schaal	X	X		5.1.1	RRE03; TPA01
5.1.2	De organisatie voert voorafgaand aan de start van een verwerking waarbij een derde partij is betrokken, een toets uit om te bepalen welke AVG-rol de eigen organisatie heeft en welke AVG-rol de derde partij heeft.	sub		In ongeveer de helft van de gevallen (≤ 65%)	schaal	X	X		5.1.5	RRE03; TPA01
5.1.3	Alvorens de organisatie een dienst (waaronder software as a service) van een verwerker inschakelt, zorgt de organisatie dat het inzicht heeft in de maatregelen ter bescherming van de persoonsgegevens van betrokkenen.	sub	Pas wanneer is vastgesteld dat de beoogde dienstverlener een adequaat niveau van privacybescherming en informatiebeveiliging kan garanderen, mag worden besloten om met deze partij een dienstverlenings- en verwerkersovereenkomst te sluiten.	In enkele gevallen (≤ 35%)	schaal	X	X		5.1.2	Leeg
5.1.4	Het uitbesteden van een verwerking van persoonsgegevens vindt uitsluitend plaats na goedkeuring daarvan door het management.	sub		In enkele gevallen (≤ 35%)	schaal	X	X		5.1.6	RRE03

5.1.5	Er worden (verwerkers)overeenkomsten afgesloten met verwerkers en gezamenlijke verwerkingsverantwoordelijken. De overeenkomsten bevatten de elementen die in de AVG zijn voorgeschreven.	sub		In ongeveer de helft van de gevallen (≤ 65%)	schaal	X	X	5.1.3	RRE03; TPA01; TPA02; DRE01
5.1.6	Het beheer van (verwerkers)overeenkomsten met verwerkers en gezamenlijke verwerkingsverantwoordelijken is in de organisatie belegd.	sub		Ja	binair			5.1.4	PP004
5.1.7	De organisatie voert periodiek een evaluatie uit van de naleving van de verplichtingen door derden. De methode is afgestemd op het risicoprofiel van de verwerking die de derde partij uitvoert.	sub	Aan de volgende methoden kan worden gedacht: a. De derde partij vult een vragenlijst in. b. De derde partij verstrekt interne auditrapporten c. De organisatie voert een evaluatie uit op locatie bij de derde partij d. De organisatie laat een audit uitvoeren bij de derde partij	In geen enkel geval (≤ 5%)	schaal			Leeg	TPA03; MON01
5.1.8	Indien de organisatie optreedt als verwerker, is er een verwerkersovereenkomst die de elementen bevat die in de AVG zijn voorgeschreven.	sub		In ongeveer de helft van de gevallen (≤ 65%)	schaal	X	X	Leeg	RRE03
5.2	Gegevensverstrekking	par	De organisatie toetst ieder voornemen om gegevens aan een derde partij te verstrekken aan de relevante privacywetten.						
5.2.1	De organisatie heeft een procedure ingericht om te waarborgen dat persoonsgegevens uitsluitend worden verstrekt aan derden als dit onder de toepasselijke (privacy)wetgeving is toegestaan.	sub	Het betreft hier verstrekking van persoonsgegevens aan een derde die het vervolgens verder verwerkt als verwerkingsverantwoordelijke.	Ja	binair			Leeg	TPD01; ULI01
5.2.2	Alvorens wordt aangevangen met een gegevensverstrekking, toetst een privacy specialist of dit in overeenstemming is met de privacywetgeving.	sub		In enkele gevallen (≤ 35%)	schaal	X	X	1.2.4; 5.2.1; 5.2.2	TPD01; ULI01
5.2.3	De organisatie documenteert in relatie tot de verstrekking: - de ontvanger; - de categorieën van persoonsgegevens; - de doeleinden; - de rechtsgrond voor verstrekking.	sub		In alle gevallen (≥ 95%)	schaal	X	X	Leeg	TPD01
5.2.4	Er wordt periodiek geëvalueerd of de verstrekkingen aan derden nog steeds in overeenstemming zijn met de wet- en regelgeving.	sub		In geen enkel geval (≤ 5%)	schaal	X	X	Leeg	ULI01
5.2.5	Alvorens de organisatie persoonsgegevens doorgeeft aan verwerkers of ontvangers in derde landen, beoordeelt de organisatie of voldaan wordt aan de wettelijke vereisten voor internationale doorgifte van persoonsgegevens.	sub	De IBD adviseert geen beroep te doen op verwerkers in derde landen waarvoor geen adequaatheidsbesluit is genomen door de Europese Commissie.	Niet van toepassing	schaal	X	X	2.6.2	DTR02
5.2.6	De organisatie heeft de verwerkingen waarbij persoonsgegevens worden overgedragen aan derde landen gedocumenteerd.	sub		Niet van toepassing	schaal	X	X	2.6.1	DTR01
5.2.7	Er wordt periodiek geëvalueerd of de doorgifte aan derde landen nog steeds in overeenstemming is met de privacywetgeving.	sub		Niet van toepassing	schaal			Leeg	Leeg
6.	Gegevensbescherming	hfd							

6.1	Risico's	par	De organisatie heeft inzicht in de risico's van de verwerking van persoonsgegevens en behandelt deze op adequate wijze.						32		
6.1.1	De organisatie heeft een beoordelingsproces voor het identificeren en aanpakken van risico's die samenhangen met het verwerken van persoonsgegevens.	sub		Ja		binair				7.2.2	RMA01; RMA03; RMA05; PBD01; ISP01; ISP03; MON02; MON03
6.1.2	De organisatie beschikt over een managementsysteem waarmee aantoonbaar de gehele Plan-Do-Check-Act cyclus op gestructureerde wijze wordt afgedekt voor wat betreft de bescherming van persoonsgegevens.	sub	Aanvulling op BIO 1.0.4zv maatregel 18.2.1.1 voor werken met persoonsgegevens.	Ja		binair				Leeg	REV01; MON01
6.2	Gegevensbescherming door ontwerp	par	Bij de ontwikkeling, het ontwerp, selectie en het gebruik van toepassingen, diensten en producten waarbij persoonsgegevens worden verwerkt, houdt de organisatie zo vroeg mogelijk in het ontwerpproces rekening met de privacybeginselen en privacyrisico's.						25 lid 1		
6.2.1	In beleid is vastgelegd dat de beoordeling van privacyrisico's en de uitvoering van de privacybeginselen aantoonbaar onderdeel is van de ontwikkeling of inkoop van producten en diensten.	sub	De privacybeginselen zijn vastgelegd in art. 5 lid 1 AVG.	Nee		binair				2.5.8; 2.5.9; 6.3.12	PBD01; PBD02
6.2.2	Voorafgaand aan de inkoop of de ontwikkeling van toepassingen, diensten en producten vindt in de praktijk daadwerkelijk een beoordeling plaats van de privacyrisico's en de maatregelen die nodig zijn om de privacybeginselen na te leven.	sub		In geen enkel geval (≤ 5%)		schaal	X	X		6.1.1; 6.1.3; 6.1.4	PBD02
6.3	Gegevensbescherming door standaardinstellingen	par	Toepassingen, diensten en producten zijn standaard ingesteld op de meest privacyvriendelijke instellingen.						25 lid 2		
6.3.1	Toepassingen, diensten en producten zijn standaard op zodanige wijze geconfigureerd dat in beginsel alleen persoonsgegevens worden verwerkt die strikt noodzakelijk zijn voor elk gespecificeerd doel van de verwerking.	sub		In enkele gevallen (≤ 35%)		schaal	X	X		6.1.5	PBD03
6.4	Informatiebeveiliging	par	De organisatie heeft passende technische en organisatorische maatregelen genomen om de beveiliging van persoonsgegevens te waarborgen.						32		
6.4.1	De organisatie heeft het informatiebeveiligingsbeleid vastgesteld.	sub		Ja		binair				Leeg	ISP05; ISP02; MON02; MON03
6.4.2	De organisatie heeft verantwoordelijkheden op het gebied van informatiebeveiliging gedefinieerd en toegewezen.	sub		In de meeste gevallen (< 95%)		schaal				Leeg	ISP01; ISP02
6.4.3	De organisatie heeft beleid, processen en procedures vastgesteld en geïmplementeerd conform de voorschriften in de BIO.	sub		In de meeste gevallen (< 95%)		schaal				Leeg	ISP01; ISP04; ISP06; ENC02; ENC03; ENC04

6.4.4	Door het uitvoeren van risicobeoordelingen heeft de organisatie vastgesteld welke technische en organisatorische beveiligingsmaatregelen noodzakelijk zijn om een passend beschermingsniveau te kunnen realiseren.	sub		In geen enkel geval (≤ 5%)	schaal	X	X	6.3.10	ISP03
6.4.5	Alle informatiesystemen waarin persoonsgegevens worden verwerkt zijn ten minste geclassificeerd op Basis Beveiligingsniveau 2 (BBN2).	sub	BBN2 is de ondergrens indien er vertrouwelijke informatie wordt verwerkt.	In alle gevallen (≥ 95%)	schaal	X	X	6.3.7	PDI01
6.4.6	Op informatiesystemen die persoonsgegevens verwerken zijn de maatregelen toegepast die horen bij het Basis Beveiligingsniveau (BBN) dat voor het systeem is vastgesteld.	sub	Voor BBN2 geldt de BIO. Voor BBN2+ heeft de IBD een aanvullend kader vastgesteld.	In alle gevallen (≥ 95%)	schaal	X	X	Leeg	ISP07; IAM01; STR01; ENC03
6.4.7	Er is een information security management system (ISMS) waarmee aantoonbaar de gehele Plan-Do-Check-Act cyclus op gestructureerde wijze wordt afgedekt.	sub	Gelijk aan BIO 1.0.4zv maatregel 18.2.1.1.	Ja	binair			6.3.5; 6.3.13	MON03
6.4.8	De organisatie beschikt over een tool om berichten en bestanden die persoonsgegevens bevatten beveiligd te verzenden. De tool ondersteunt ten minste de volgende functionaliteiten: - Versleuteling van verbindingen en inhoud; - Verificatie van ontvangers.	sub	Aanvulling op BIO 1.0.4zv maatregel 13.2.3 voor werken met persoonsgegevens.	Ja	binair			Leeg	STR01
6.4.9	In beleid is vastgelegd dat het verboden is om persoonsgegevens die de organisatie onder zich heeft op te slaan op apparaten die niet door de organisatie worden beheerd of zijn goedgekeurd.	sub	Denk hierbij bijvoorbeeld aan apparaten die eigendom zijn van medewerkers, zoals smartphones en USB-sticks.	Nee	binair			Leeg	ENC01
6.4.10	Wanneer de handelingen van medewerkers in een systeem worden gelogd ten behoeve van gegevensbescherming, worden medewerkers hiervan tijdig op de hoogte gebracht.	sub	Aanvulling op BIO 1.0.4zv maatregel 12.4.1 voor werken met persoonsgegevens.	In alle gevallen (≥ 95%)	schaal	X	X	3.4.4	LOG01
6.5	Privacyincidenten en datalekken	par	De organisatie detecteert en behandelt privacygerelateerde incidenten op systematische wijze.					33; 34	
6.5.1	De organisatie heeft een proces vastgesteld voor het detecteren en afhandelen van privacyincidenten.	sub	Het is aanbevelenswaardig om dit te integreren met het algemene incidentmanagementproces van de organisatie.	Ja	binair			6.2.4	PIB01; ENC04
6.5.2	Het privacyincidentenproces bepaalt: 1. via welk kanaal en binnen welk tijdspad medewerkers een (vermoed) privacyincident dienen te melden; 2. welke functionaris bepaalt of het privacyincident een inbreuk in verband met persoonsgegevens (datalek) betreft dat moet worden gemeld aan de AP en in voorkomend geval aan betrokkenen; 3. wie verantwoordelijk is voor het coördineren van de afhandeling van het privacyincident; 4. de documentatievereisten bij het afhandelen van een privacyincident.	sub		Ja	binair			Leeg	PIB01; PIB03; PIB05
6.5.3	Het privacyincidentenproces bepaalt wie verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.	sub		Ja	binair			Leeg	PIB06

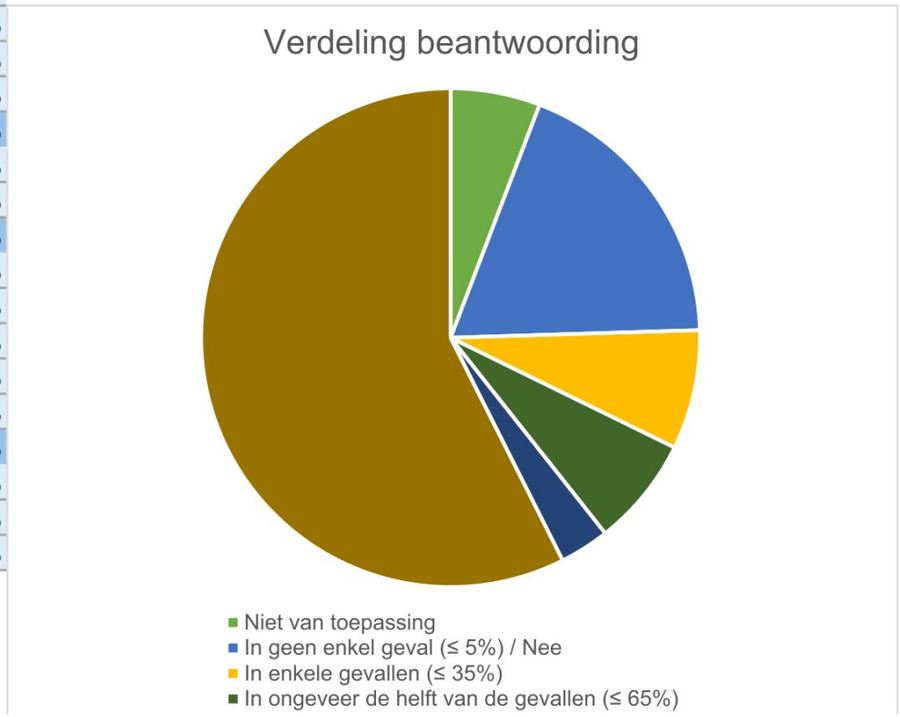
6.5.4	Het privacyincidentenproces geeft een afwegingskader omtrent het al dan niet melden van een inbreuk in verband met persoonsgegevens (datalek) aan de AP.	sub		Ja	binair			6.2.3	PIB04
6.5.5	Het privacyincidentenproces bepaalt wie verantwoordelijk is voor het melden van een datalek bij betrokkenen.	sub		Ja	binair			6.2.5	Leeg
6.5.6	Het privacyincidentenproces geeft een afwegingskader omtrent het al dan niet melden van datalekken aan betrokkenen.	sub		Ja	binair			6.2.3	Leeg
6.5.7	De organisatie heeft voor zowel interne als externe doelgroepen een meldpunt voor privacyincidenten.	sub	Dit mogen verschillende kanalen zijn (intern en extern). Interne doelgroepen zijn bijv. medewerkers. Externe doelgroepen zijn bijv. verwerkers of klanten.	Ja	binair			Leeg	PIB01
6.5.8	Als onderdeel van het bewustwordingsprogramma worden medewerkers bekend gemaakt met hun verantwoordelijkheden ten aanzien van privacyincidenten.	sub		Ja	binair	X		6.2.1; 6.2.2	PIB07
6.5.9	De organisatie is in staat om een inbreuk in verband met persoonsgegevens (datalek) tijdig bij de AP te melden.	sub		In alle gevallen (≥ 95%)	schaal			Leeg	Leeg
6.5.10	Het SOC (security operations center) heeft heldere regels over wanneer een incident als privacyincident moet worden aangemerkt en opgevolgd.	sub	Aanvulling op BIO 1.0.4zv maatregel 12.4.1 voor werken met persoonsgegevens.	Ja	binair			Leeg	PIB01
6.5.11	Als onderdeel van het privacyincidentenproces wordt na ieder privacyincident een evaluatie uitgevoerd om correcties en verbeteringen te identificeren.	sub		In alle gevallen (≥ 95%)	schaal			Leeg	PIB08; PIB09
6.5.12	De resultaten van de evaluatie van een privacyincident worden aan het management gecommuniceerd.	sub		In alle gevallen (≥ 95%)	schaal			Leeg	PIB08
6.5.13	Er is een crisiscommunicatieplan voor datalekken met hoge impact.	sub		Ja	binair			6.2.8	PIB03
7.	Verantwoording	hfd							
7.1	Evaluatie naleving AVG	par	Zowel het management als de FG controleren de naleving van de AVG doorlopend.						
7.1.1	Periodiek wordt, onder aansturing van het management, de naleving van de AVG bij de uitvoering van de taken van het management geëvalueerd.	sub	Het management heeft de verantwoordelijkheid voor privacybescherming bij de uitvoering van hun taken. Daarom is het van belang dat het management zelf een beeld vormt van de mate waarin privacywetgeving wordt nageleefd. Het management kan zich hierin laten ondersteunen door een privacy specialist. Deze controles staan los van het onafhankelijke toezicht van de FG.	Nee	binair	X	X	7.4.1	Leeg
7.1.2	De FG heeft een toezichtplan om als onafhankelijk toezichthouder de naleving van de AVG door de organisatie te controleren.	sub	Deze controles behoren onafhankelijk van het management te worden verricht.	Nee	binair			3.1.9; 7.1.2	REV01
7.1.3	De FG controleert in de praktijk daadwerkelijk de naleving van de AVG door de organisatie.	sub	Dit kan bijv. getoetst worden aan de hand van initiatieven die de FG neemt, zoals memo's die zijn opgesteld n.a.v. toezichtsacties en bevragingen over naleving.	Nee	binair			3.1.7	REV01
7.1.4	De organisatie volgt afwijkingen die zijn geconstateerd bij een evaluatie van de naleving van de AVG gestructureerd op.	sub	Deze maatregel betreft het opvolgen van gebreken in de naleving van de AVG die zijn geconstateerd n.a.v. evaluaties uitgevoerd onder verantwoordelijkheid van het management of door de FG.	In geen enkel geval (≤ 5%)	schaal	X	X	7.4.2	Leeg

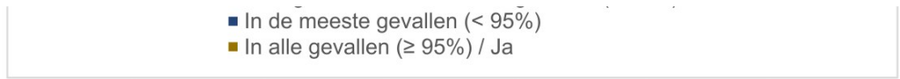
7.2	Evaluatie informatiebeveiliging	par	De mate waarin de doelstellingen van het informatiebeveiligingsbeleid worden bereikt wordt doorlopend gecontroleerd.									
7.2.1	Periodiek wordt de uitvoering van het informatiebeveiligingsbeleid en de naleving van processen, procedures en standaarden geëvalueerd.	sub		Ja		binair	X			Leeg	ISP05; REV01
7.2.2	Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of penetratietesten.	sub	Gelijk aan BIO 1.0.4zv maatregel 18.2.3.1.	Ja		binair	X	X		Leeg	MON02
7.3	Rapportage	par	Periodiek worden interne en externe stakeholders op de hoogte gehouden over de naleving van de AVG door de organisatie.						39		
7.3.1	Middels een jaarverslag wordt het management en het bestuursorgaan geïnformeerd over de naleving van de AVG door de organisatie. De FG is verantwoordelijk voor dit jaarverslag.	sub		Ja		binair				6.3.13; 6.3.14; 7.3.4	REV01

Borgingsproduct AVG v3.0
Dashboard

	Naam organisatie		Gemeente Dalfsen		
	Datum ingevuld		19 maart 2025		
	Aantal beantwoord		146 van de 155		
	Score		69%		
Par	Titel	Leeg	N.v.t	Beantwoord	Percentage
1.	Beleid	0	0	0	0%
1.1	Beleid vaststellen	0	0	0	0%
1.2	Privacybeleid	0	0	0	0%
1.3	Verantwoordelijkheden	0	0	0	0%
2.	Processen	0	0	0	0%
2.1	Werkprocessen	0	0	0	0%
2.2	Verwerkingsregister	0	0	0	0%
2.3	Pre-DPIA's	0	0	0	0%
2.4	DPIA's	0	0	0	0%
2.5	Bewaar- en vernietigingsbeleid	0	0	0	0%
3.	Organisatorische inbedding	0	0	0	0%
3.1	Privacyteam	0	0	0	0%
3.2	Aanstelling, positie en taken FG	0	0	0	0%
3.3	Informeren OR	0	0	0	0%
3.4	Bewustwording	0	0	0	0%
4.	Rechten van betrokkenen	0	0	0	0%
4.1	Recht op informatie	0	0	0	0%
4.2	Processen rechten van betrokkenen	0	0	0	0%
4.3	Toestemming	0	0	0	0%
4.4	Geautomatiseerde individuele besluitvorming	0	0	0	0%
4.5	Websites en applicaties	0	0	0	0%
4.6	Technische ondersteuning	0	0	0	0%
5.	Samenwerking	0	0	0	0%
5.1	AVG rollen	0	0	0	0%
5.2	Gegevensverstrekking	0	0	0	0%
6.	Gegevensbescherming	0	0	0	0%
6.1	Risico's	0	0	0	0%
6.2	Gegevensbescherming door ontwerp	0	0	0	0%
6.3	Gegevensbescherming door standaardinstellingen	0	0	0	0%
6.4	Informatiebeveiliging	0	0	0	0%
6.5	Privacyincidenten en datalekken	0	0	0	0%
7.	Verantwoording	0	0	0	0%
7.1	Evaluatie naleving AVG	0	0	0	0%
7.2	Evaluatie informatiebeveiliging	0	0	0	0%
7.3	Rapportage	0	0	0	0%

INFORMATIE BEVEILIGINGS DIENST




In de meeste gevallen (< 95%)
In alle gevallen (≥ 95%) / Ja