

INHOUD

VOORWOORD	15
LIJST VAN AFKORTINGEN	21
1 ALGEMENE INLEIDING	23
1.1 Inleiding	24
1.2 Erkenning van de FG in de AVG	25
1.3 Aanstellen van een FG	25
1.3.1 Historische ervaringen met de FG	26
1.3.2 Facultatieve benoeming conform de Wbp	26
1.3.3 Verplichte aanwijzing conform de AVG	27
1.3.3.1 Overheidsinstantie of overheidsorgaan	28
1.3.3.2 Hoofdzakelijk belast met (kerntaken)	28
1.3.3.3 Op grote schaal	29
1.3.3.4 Regelmatige en stelselmatige observatie	31
1.3.3.5 Speciale gegevenscategorieën: strafrechtelijke gegevens	32
1.3.4 FG van de verwerker	32
1.3.5 Een FG voor meerdere organisaties	33
1.3.5.1 Ondersteuning door een FG-team	33
1.3.5.2 Een FG voor verschillende overheidsinstanties of overheidsorganen	34
1.3.6 Operationele aspecten vanwege de FG aanwijzing	34
1.3.7 Eisen aan de FG onder de AVG	35
1.3.7.1 Professionele kwaliteiten	35
1.3.7.2 Deskundigheid op het gebied van de wetgeving	36
1.3.7.3 Deskundigheid van de praktijk inzake gegevensbescherming	36
1.3.7.4 Het vermogen om de volgende (in artikel 39 AVG genoemde) taken te vervullen	36
1.3.7.5 FG op basis van een dienstverleningsovereenkomst (externe FG)	37
1.3.8 Facultatieve (vrijwillige) aanwijzing conform de AVG	38
1.4 Taken van de FG onder de Wbp	39
2 TAKEN, POSITIONERING EN FUNCTIEPROFIEL VAN DE FG	41
2.1 Wettelijke taken (AVG)	42
2.2 Optionele taken	45
2.3 Taakgerichte bevoegdheden	46
2.4 Positionering	46
2.4.1 Wettelijke eisen aan de positionering, WBP	46
2.4.2 Wettelijke eisen aan de positionering, AVG	46
2.4.3 Positionering van de FG als line of defense	52
2.4.4 Taakgerichte (operationele) positionering	52
2.5 Functieprofiel van de FG	53
2.5.1 Functieanalyse van de FG	53
2.5.2 Functieprofiel: positionering van de FG	55

2.5.3	Functieprofiel: competentieprofiel	56
2.5.3.1	Integriteit en geloofwaardigheid van de FG	56
2.5.3.2	Emotionele competentie van de FG	56
2.5.3.3	Leiderschap van de FG	57
2.5.3.4	Rollenmatrix competenties van de FG	58
2.5.3.5	Andere manieren van het profileren van de functie van FG	60
2.5.3.6	Biografische vragenlijsten	60
2.5.4	Recruitment (werving en selectie) van de geschikte FG	61
2.6	Oriëntatietabel FG-functiemodel	63
3	FG-WERKPROGRAMMA: OPZET EN STRUCTUUR	67
3.1	Inleiding	68
3.1.1	Werkprogramma van de FG	68
3.1.2	Drivers voor een FG-werkprogramma	68
3.1.3	Business case voor een professioneel FG-werkprogramma	70
3.1.3.1	Baten (rechtvaardiging)	70
3.1.3.2	Kosten	75
3.1.4	Behandelplan	77
3.2	Vertrekpunten voor de opzet en structuur van een FG-werkprogramma	78
3.2.1	AVG-opdracht aan de FG	78
3.2.2	AVG-conforme positionering	79
3.2.3	Multidisciplinaire perspectieven	80
3.2.4	AVG-kernthema's van het FG-werkprogramma	81
3.2.5	Ontologie van het FG-werkprogramma	82
3.2.6	Ondersteuning met benodigde middelen	83
3.2.7	Planning	83
3.2.7.1	Korte termijn (prioriteitenmatrix van Eisenhower)	84
3.2.7.2	Lange termijn (maturiteitsmodel)	85
3.3	Opzet van een FG-werkprogramma	86
3.3.1	Basisopzet van een FG-werkprogramma	86
3.3.2	Inhoudelijke eisen aan een FG-werkprogramma	87
3.3.2.1	AVG	87
3.3.2.2	Andere Unierechtelijke gegevensbeschermingsbepalingen	88
3.3.2.3	Nederlandsrechtelijke gegevensbeschermingsbepalingen	88
3.3.2.4	Organisatiespecifieke (interne) regelingen	88
3.3.3	Risico-oriëntatie in het FG-werkprogramma	88
3.3.3.1	COSO-ERM risicomanagement model	89
3.3.3.2	Elementen van risicobeheersing	90
3.3.3.3	FG PRISC-model ®	90
3.3.4	Reikwijdte van het FG-werkprogramma	91
3.3.5	Succesfactoren voor een professioneel FG-werkprogramma	92
3.4	Structuur van een professioneel FG-werkprogramma	93
3.4.1	Basisstructuur van een FG-werkprogramma	93
3.4.2	Zes strategische pijlers van het FG-werkprogramma	93
3.4.2.1	Pijler 1: informeren en adviseren	94
3.4.2.2	Pijler 2: toezien op de naleving	95
3.4.2.3	Pijler 3: samenwerken met de AP	96

3.4.2.4	Pijler 4: contactpunt voor de Autoriteit Persoonsgegevens	97
3.4.2.5	Pijler 5: contactpunt voor betrokkenen	98
3.4.2.6	Pijler 6: andere (optionele) taken	98
3.4.3	Stappenplan voor FG-toezien op AVG-compliance	100
3.5	Roadmap opzet en structuur FG-werkprogramma	100
4	VISIE, MISSIE EN STRATEGIE	103
4.1	Inleiding	104
4.1.1	Visie, missie en strategie van een professioneel werkprogramma van de FG	104
4.1.2	Bepalen van de visie van het FG-werkprogramma	105
4.1.3	De missie van het FG-werkprogramma	106
4.1.4	Strategie van het FG-werkprogramma	106
4.1.5	VMS calibratie van het FG-werkprogramma	107
4.1.6	Plan van behandeling van dit hoofdstuk	108
4.2	Stakeholders VMS van het FG-werkprogramma	109
4.2.1	De Europese wetgever en VMS van het FG-werkprogramma	109
4.2.2	Europese Commissie en VMS van het FG-werkprogramma	111
4.2.3	De European Data Protection Supervisor (EDPS)	116
4.2.4	De Nederlandse wetgever en VMS van het FG-werkprogramma	118
4.2.5	Europees Comité en VMS van het FG-werkprogramma	120
4.2.6	Autoriteit Persoonsgegevens en VMS van het FG-werkprogramma	122
4.2.7	Beroepsgroep FG'S en VMS van het FG-werkprogramma	123
4.2.8	Verwerkingsverantwoordelijke en VMS van het FG-werkprogramma	126
4.2.9	FG ex professio en VMS van het FG-werkprogramma	128
4.2.10	Interne stakeholders en VMS van het FG-werkprogramma	129
4.3	Oriëntatietabel FG-werkprogramma: visie, missie en strategie	131
5	FG-WERKPROGRAMMA: INVENTARISATIE VAN VERWERKINGEN	139
5.1	Inleiding	140
5.1.1	Definitie van inventariseren	140
5.1.2	Ratio en doel van inventarisatie	140
5.1.3	Persoonsgegevens behoren tot de DNA van de organisatie	141
5.1.4	Persoonsgegevens en business intelligence	141
5.1.5	Inventariseren van persoonsgegevens in de AVG	142
5.1.6	Algemene AVG-privacy zorgplicht van de verwerkingsverantwoordelijke	144
5.1.7	FG-belang bij het inventariseren van persoonsgegevens	144
5.1.8	Effectueren rechten van betrokkenen	145
5.1.9	Fuik van de privacyabstractie	146
5.1.10	Behandelplan	148
5.2	Inventarisatie van persoonsgegevens: doelen en neveneffecten	148
5.2.1	Algemene doelen van een AVG-inventarisatie	148
5.2.1.1	Compliance (art. 30 lid 1 AVG)	149
5.2.1.2	Compliance (art. 35 AVG)	150
5.2.1.3	Nakomen AVG-privacy zorgplicht (art. 5 lid 1 AVG)	151
5.2.1.4	Effectueren rechten van betrokkenen (hoofdstuk III AVG)	152
5.2.2	Neveneffecten van een AVG-inventarisatie	153
5.2.2.1	Bevordert privacy awareness (art. 39 lid 1 onder b AVG)	153

5.2.2.2	Uitvoeren passende en effectieve maatregelen	153
5.2.2.3	Verminderen van de kans op een klacht	154
5.2.2.4	Beperken aansprakelijkheid (art. 82 AVG)	154
5.3	Inventarisatie van persoonsgegevens processtappen	155
5.3.1	Stap 1: stel het doel van de inventarisatie vast	155
5.3.2	Stap 2: bepaal de scope van de inventarisatie	155
5.3.3	Stap 3: maak een Data Inventarisatie Template (DIT)	158
5.3.4	Stap 4: identificeer bronnen van persoonsgegevens	158
5.3.5	Stap 5: vul DIT in	159
5.3.6	Personal Data Process Flow (PDPF)	159
5.3.7	Data kwaliteitsmanagement	161
5.3.8	Ondersteuning door IT	161
5.4	Inventarisatie van persoonsgegevens	161
5.4.1	Waarom een inventarisatieplan	161
5.4.2	Roadmap van een inventarisatieplan	162
5.4.2.1	Inventarisatiemandaat	163
5.4.2.2	Inventarisatieteam	163
5.4.2.3	Uitvoeren inventarisatieproject	164
5.4.2.4	Stakeholdersmanagement	165
5.4.2.5	Evaluatie- en actualisatieplan	166
5.4.2.6	Eindrapportage (art. 5 lid 2 AVG)	166
5.4.3	Succesfactoren voor een goed inventarisatieplan	167
5.5	Rol van de FG bij inventarisatie van persoonsgegevens	167
5.6	Oriëntatietabel FG-werkprogramma: AVG-inventarisatie	169
6	FG-WERKPROGRAMMA: AVG-NULMETING EN AVG-GAP-ANALYSE	179
6.1	Inleiding	180
6.1.1	Definities van een AVG-nulmeting en AVG-gap-analyse	180
6.1.2	Ratio van een AVG-nulmeting en AVG-gap-analyse	181
6.1.3	Doelen en neveneffecten van een AVG-nulmeting en AVG-gap-analyse	182
6.1.3.1	Algemene doelen van een AVG-nulmeting en AVG-gap-analyse	182
6.1.3.1.1	Input passend gegevensbeschermingsbeleid (art. 24 lid 2 AVG)	183
6.1.3.1.2	Input voor passende en effectieve maatregelen	183
6.1.3.1.3	Controle doelbinding (art. 5 lid 1 onder b AVG)	184
6.1.3.1.4	Concretiseren AVG-privacy zorgplicht compliance	184
6.1.3.1.5	Registerplicht (art. 30 AVG)	185
6.1.3.1.6	Beheersen van processen (requirements en controls)	186
6.1.3.1.7	Risk management en control	186
6.1.3.1.8	Issue management	187
6.1.3.1.9	Data Protection Impact Assessment	187
6.1.3.1.10	Verantwoordingsplicht (art. 5 lid 2 AVG)	188
6.1.3.2	Neveneffecten van een AVG-nulmeting en AVG-gap-analyse	189
6.1.3.2.1	Bevorderen privacy awareness (art. 39 lid 1 onder b AVG)	189
6.1.3.2.2	Bevorderen inzicht in aantal verwerkingen en verwerkingsprocessen	190
6.1.3.2.3	Bevorderen inzicht in het belang van verwerkingen voor kernprocessen	191
6.1.3.2.4	Bevorderen effectiever toezien door de FG (art. 39 lid 2 AVG)	192
6.1.3.2.5	Bevorderen inzicht in benodigde middelen voor de FG (art. 38 lid 2 AVG)	193

6.1.4	Ideaal team voor een AVG-nulmeting en AVG-gap-analyse	193
6.1.5	Managementwaarde van een AVG-nulmeting en AVG-gap-analyse	196
6.1.6	Parameters van de AVG-nulmeting en de AVG-gap-analyse	196
6.1.7	Verschillen tussen een AVG-nulmeting en AVG-gap-analyse	198
6.1.8	Taxonomie van verplichtingen uit hoofde van de AVG	198
6.1.8.1	Grondrechten en fundamentele vrijheden	199
6.1.8.2	Definitie van persoonsgegevens	201
6.1.8.3	AVG-compliance pyramide	203
6.1.9	Belang van de FG bij een AVG-nulmeting en AVG-gap-analyse	203
6.1.10	Behandelplan	204
6.2	AVG-nulmeting: processtappen	205
6.2.1	Stap 1: bepaal de doelen van de AVG-nulmeting	205
6.2.2	Stap 2: bepaal de scope van de AVG-nulmeting	209
6.2.3	Stap 3: benoem de bestanddelen van de desbetreffende AVG-verplichting(en)	211
6.2.4	Stap 4: stel per bestanddeel de relevante parameters vast (maak een map)	212
6.2.5	Stap 5: stel per parameter vast de actie wel of niet is uitgevoerd	213
6.2.6	Stap 6: bereken de totale compliancewaarden en stel de compliancestatus vast van de AVG-verplichting	213
6.2.7	Leg alle stappen vast in een overzichtelijk verantwoordingsmodel (ABC-model)	214
6.2.8	Maak gebruik van in de organisatie aanwezige kennis en (IT-)expertise	214
6.2.9	Kwaliteitsvraagstukken	216
6.2.10	AVG-nulmeting in perspectief	216
6.3	AVG-gap-analyse: processtappen	217
6.3.1	Logische processtappen van een AVG-gap-analyse	217
6.3.1.1	Vaststellen van het AVG-compliance ambitieniveau (STAP)	218
6.3.1.2	Per stap aangegeuide concrete actie (STIP)	219
6.3.1.3	STIP AVG-compliance monitor	221
6.3.2	Processtappen van een AVG-gap-analyse	222
6.3.3	Stap 1: bepaal het doel van de AVG-gap-analyse	223
6.3.4	Stap 2: bepaal de scope van de AVG-gap-analyse	223
6.3.5	Stap 3: stel het Gap Analysis Template (GAT) samen	224
6.3.6	Stap 4: vul het AVG-ambitieniveau in het GAT in	225
6.3.7	Stap 5: specificeer de maatregelen in het GAT	225
6.3.8	Stap 6: vul de (uit te voeren) acties in het GAT in	226
6.3.9	Een overzichtelijk AVG-implementatieplan	226
6.3.10	AVG-gap-analyse en data governance	226
6.3.11	Organiseer kennis en (IT) expertise	226
6.3.12	Ratio en geest van AVG-maatregelen en acties	226
6.4	AVG-nulmeting en AVG-gap-analyse: roadmap	227
6.4.1	Waarom een roadmap voor de AVG-nulmeting en AVG-gap-analyse?	227
6.4.2	Roadmap van een AVG-nulmeting en AVG-gap-analyse	228
6.4.2.1	Mandaat voor de AVG-nulmeting en AVG-gap-analyse	228
6.4.2.2	Samenstellen team voor het uitvoeren van de AVG-nulmeting en AVG-gap-analyse	229
6.4.2.3	Uitvoeren van de AVG-nulmeting en AVG-gap-analyse	229

6.4.2.4	Stakeholdersmanagement	231
6.4.2.5	Evaluatie en actualisatieplan (EAP)	232
6.4.2.6	AVG-eindrapportage en AVG-verantwoording (art. 5 lid 2 AVG)	233
6.5	Succesfactoren voor een AVG-nulmeting en AVG-gap-analyse	233
6.6	Rol van de FG bij een AVG-nulmeting en AVG-gap-analyse	234
6.7	Oriëntatietabel FG-werkprogramma: AVG-nulmeting en AVG-gap-analyse	235
7	FG-WERKPROGRAMMA: AVG-IMPLEMENTATIEPLAN	255
7.1	Inleiding AVG-implementatieplan	256
7.1.1	Wat is een AVG-implementatieplan (AIP)?	256
7.1.2	Ratio van een AIP	256
7.1.3	Doelen van een AIP	257
7.1.4	Reikwijdte (scope) van een AIP	257
7.1.5	Logische processtappen van het AIP	258
7.1.6	Ideaal team voor een AIP	258
7.1.7	Managementwaarde van een AIP	260
7.1.8	Belang van de FG bij een goed AIP	260
7.1.9	Behandelplan	261
7.2	AIP: doelen en neveneffecten	262
7.2.1	Algemene doelen van een AIP	262
7.2.1.1	Uitvoeren passend gegevensbeschermingsbeleid (art. 24 lid 2 AVG)	263
7.2.1.2	Treffen passende en effectieve maatregelen	263
7.2.1.3	Concretisering en naleving van AVG-beginselen (art. 5 lid 1 AVG)	264
7.2.1.4	Bewaken van rechtmatige grondslag (art. 6 AVG)	264
7.2.1.5	Houden van een register van de verwerkingsactiviteiten ex art. 30 AVG	265
7.2.1.6	Implementeren van AVG-requirements en AVG-controls	266
7.2.1.7	Realiseren AVG-risk management en control	267
7.2.1.8	Realiseren AVG-issue management	267
7.2.1.9	Naleven Data Protection Impact Assessment (DPIA) plicht	267
7.2.1.10	Naleven AVG-compliance en accountability plicht (art. 5 lid 2 AVG)	268
7.2.2	Neveneffecten van een AIP	268
7.3	AIP: processtappen	269
7.3.1	Stap 1: stel een AVG-implementatieteam samen	269
7.3.2	Stap 2: bepaal wat moet worden geïmplementeerd	270
7.3.3	Stap 3: definieer hetgeen moet worden geïmplementeerd	271
7.3.4	Stap 4: ontwerp hetgeen moet worden geïmplementeerd	271
7.3.5	Stap 5: test werking en effectiviteit van de maatregelen	271
7.3.6	Stap 6: bewijsrapportage van de getroffen AVG-maatregelen	272
7.3.7	Een overzichtelijk AIP	272
7.3.8	Organiseer kennis en (IT) expertise	273
7.4	AIP: roadmap	273
7.4.1	Waarom een roadmap voor het AIP?	273
7.4.2	Roadmap van een AIP	274
7.4.2.1	Mandaat en stuurinformatie voor het AIP	274
7.4.2.2	Operationaliseren van het AIP	275
7.4.2.3	Managen van verwachtingen van stakeholders	275
7.4.2.4	Uitvoeren van concrete acties	276

7.4.2.5	Evaluatie en actualisatieplan (EAP)	276
7.4.2.6	Uitvoeringsrapportage van het AIP (art. 5 lid 2 AVG)	277
7.4.3	Succesfactoren voor een AIP	277
7.5	AIP: rol van de FG	278
7.6	Oriëntatietabel FG-werkprogramma: AVG-implementatie	279
8	FG-WERKPROGRAMMA: EVALUATIE EN ACTUALISATIE	291
8.1	Inleiding AVG-evaluatie- en actualisatieplan	292
8.1.1	Wat is een AVG-evaluatie- en actualisatieplan (EAP)?	292
8.1.2	Ratio van een EAP	293
8.1.3	Doelen van een EAP	293
8.1.4	Reikwijdte (scope) van een EAP	293
8.1.5	Logische procesfasen EAP	294
8.1.6	Het ideale team voor AVG-evaluatie en -actualisatie	294
8.1.7	Managementwaarde van een EAP	295
8.1.8	Belang van de FG bij een goed EAP	295
8.1.9	Behandelplan	296
8.2	EAP: doelen en neveneffecten	297
8.2.1	Algemene doelen van een EAP	297
8.2.1.1	Realiseren passend en effectief gegevensbeschermingsbeleid (art. 24 leden 1 en 2 AVG)	297
8.2.1.2	Realiseren passende en effectieve maatregelen	298
8.2.1.3	Nadere concretisering en naleving van de AVG-privacy zorgplicht (art. 5 lid 1 AVG)	298
8.2.1.4	Nadere concretisering rechtmatigheid (art. 6 AVG)	299
8.2.1.5	Realiseren van een actueel register van verwerkingsactiviteiten ex art. 30 AVG	300
8.2.1.6	Up-to-date beheersen van processen (AVG-requirements en AVG-controls)	300
8.2.1.7	Realiseren van effectief AVG-risk management en control	301
8.2.1.8	Realiseren van effectief issue management	301
8.2.1.9	Effectief naleven Data Protection Impact Assessment (DPIA) verplichting	302
8.2.1.10	Effectief naleven AVG-compliance en accountability plichten (art. 5 lid 2 AVG)	302
8.2.2	Neveneffecten van een EAP	303
8.3	AVG-evaluatieplan (AEP): processtappen	304
8.3.1	Stap 1: stel een AVG-evaluatieteam samen	304
8.3.2	Stap 2: bepaal welke AVG-onderdelen moeten worden geëvalueerd	304
8.3.3	Stap 3: definieer hetgeen moet worden geëvalueerd	305
8.3.4	Stap 4: stel de AVG-evaluatiecriteria vast	305
8.3.5	Stap 5: voer de feitelijke AVG-evaluatie uit	306
8.3.6	Stap 6: rapporteer over de feitelijk uitgevoerde AVG-evaluatie	306
8.3.7	Een overzichtelijk AVG-evaluatieplan (AEP)	306
8.3.8	Organiseer kennis en expertise rondom evaluatie	306
8.4	AVG-actualisatieplan (AAP): processtappen	307
8.4.1	Stap 1: stel een AVG-actualisatieteam samen	307
8.4.2	Stap 2: bepaal welke AVG-maatregelen/acties moeten worden geactualiseerd	308

8.4.3	Stap 3: definieer hetgeen moet worden geactualiseerd	308
8.4.4	Stap 4: stel de AVG-actualisatie-eisen vast	308
8.4.5	Stap 5: voer de feitelijke AVG-actualisatie uit	309
8.4.6	Stap 6: rapporteer over de feitelijk uitgevoerde AVG-actualisatie	309
8.4.7	Een overzichtelijk AAP	309
8.4.8	Organiseer kennis en expertise rondom AVG-actualisatie	309
8.5	AVG-evaluatie- en actualisatieplan (EAP): roadmap	309
8.5.1	Waarom een roadmap voor het EAP?	309
8.5.2	Roadmap van een EAP	311
8.5.2.1	Mandaat en stuurinformatie voor het AVG-evaluatie- en actualisatieteam	311
8.5.2.2	Samenstellen team voor uitvoering van het EAP	311
8.5.2.3	Inbedden van stakeholdersmanagement	311
8.5.2.4	Vaststellen risico-oriëntatie in het EAP	312
8.5.2.5	Tussentijds rapporteren	312
8.5.2.6	Samenstellen EAP-eindrapportage (art. 5 lid 2 AVG)	312
8.5.3	Succesfactoren voor de goede uitvoering van een EAP	312
8.6	AVG-evaluatie- en actualisatieplan (EAP): rol FG	312
8.7	Oriëntatietabel FG-werkprogramma: AVG-evaluatie en AVG-actualisatie	315
9	FG-WERKPROGRAMMA: AVG-ASSURANCE EN AVG-AUDIT	335
9.1	Inleiding AVG-assurance en AVG-audit	336
9.1.1	Wat is AVG-assurance en AVG-audit	336
9.1.2	Ratio van AVG-assurance en AVG-audit	338
9.1.3	Doelen van AVG-assurance en AVG-audit	338
9.1.4	Reikwijdte (scope) van AVG-assurance en AVG-audit	339
9.1.5	Logische procesfasen van AVG-assurance en AVG-audit	339
9.1.6	Ideale teams voor AVG-assurance en AVG-audits	340
9.1.7	Managementwaarde van AVG-assurance en AVG-audits	340
9.1.8	Belang van de FG bij AVG-assurance en AVG-audits	340
9.1.9	Behandelplan	341
9.2	AVG-assurance en AVG-audits: doelen en neveneffecten	342
9.2.1	Algemene doelen van AVG-assurance en AVG-audits	342
9.2.1.1	Nalevingscontrole passend en effectief gegevensbeschermingsbeleid (art. 24 leden 1 en 2 AVG)	343
9.2.1.2	Nalevingscontrole passende en effectieve maatregelen	343
9.2.1.3	Nalevingscontrole concretisering en naleving algemene AVG-zorgplicht (art. 5 lid 1 AVG)	344
9.2.1.4	Nalevingscontrole concretisering rechtmatigheid (art. 6 AVG)	344
9.2.1.5	Nalevingscontrole actueel register ex art. 30 AVG	345
9.2.1.6	Nalevingscontrole beheersen van processen (AVG-requirements en AVG-controls)	346
9.2.1.7	Nalevingscontrole effectief AVG-risk management & control	346
9.2.1.8	Nalevingscontrole effectief AVG-issue management	347
9.2.1.9	Nalevingscontrole Data Protection Impact Assessment (DPIA) verplichting	347
9.2.1.10	Nalevingscontrole verantwoordingsplicht (art. 5 lid 2 AVG)	347
9.2.1.11	Neveneffecten van AVG-assurance en AVG-audit	348

9.3	AVG-assurance: processtappen	349
9.3.1	Stap 1: stel een AVG-assuranceteam samen	349
9.3.2	Stap 2: bepaal het subject van de AVG-assurance	349
9.3.3	Stap 3: stel de scope van de AVG-assurance vast	350
9.3.4	Stap 4: stel de te hanteren AVG-toetsingcriteria vast	350
9.3.5	Stap 5: voer de feitelijke AVG-assurance-activiteiten uit	351
9.3.6	Stap 6: rapporteer over de uitgevoerde AVG-assurance-activiteiten	351
9.3.7	Een overzichtelijk AVG-assuranceplan	351
9.3.8	Organiseer kennis en expertise rondom AVG-assurance	351
9.4	AVG-assurance: roadmap	352
9.4.1	Waarom een roadmap voor AVG-assurance?	352
9.4.2	Roadmap AVG-assurance	353
9.4.2.1	Mandaat voor AVG-assurance	353
9.4.2.2	Samenstellen AVG-assuranceteam	353
9.4.2.3	Inbedden van AVG-stakeholdersmanagement	353
9.4.2.4	Vaststellen risico-oriëntatie AVG-assurance	354
9.4.2.5	Tussentijds rapporteren over AVG-assurance	354
9.4.2.6	Samenstellen eindrapportage AVG-assurance (art. 5 lid 2 AVG)	354
9.4.3	Succesfactoren voor de goede uitvoering van AVG-assurance	354
9.5	AVG-audit: processtappen	355
9.5.1	Stap 1: stel een AVG-auditteam samen	355
9.5.2	Stap 2: bepaal het subject van de AVG-audit	355
9.5.3	Stap 3: stel de scope van de AVG-audit vast	356
9.5.4	Stap 4: stel de te hanteren AVG-auditcriteria vast	356
9.5.5	Stap 5: voer de feitelijke AVG-auditactiviteiten uit	356
9.5.6	Stap 6: rapporteer over de uitgevoerde AVG-auditactiviteiten	357
9.5.7	Een overzichtelijk AVG-audit(stappen)plan	357
9.5.8	Organiseer kennis en expertise rondom de AVG-audit	357
9.6	AVG-audit: roadmap	357
9.6.1	Waarom een roadmap voor AVG-audits?	357
9.6.2	Roadmap van de AVG-audit	359
9.6.2.1	Mandaat voor het uitvoeren van de AVG-audit	359
9.6.2.2	Samenstellen AVG-auditteam	359
9.6.2.3	Inbedden van AVG-stakeholdersmanagement	359
9.6.2.4	Vaststellen risico-oriëntatie van de AVG-audit	360
9.6.2.5	Tussentijds rapporteren over de AVG-audit	360
9.6.2.6	Samenstellen eindrapportage van de AVG-audit (art. 5 lid 2 AVG)	360
9.6.3	Succesfactoren voor de goede uitvoering van AVG-audits	360
9.7	AVG-assurance en AVG-audits: rol van de FG (DPO)	361
9.8	Oriëntatietabel FG-werkprogramma: AVG-assurance en AVG-audit	363
10	FG-WERKPROGRAMMA: VERANTWOORDING EN RAPPORTAGE	383
10.1	Inleiding verantwoording en rapportage in de AVG	384
10.1.1	Een Verantwoording en Rapportageplan (VRP)	384
10.1.2	Ratio van een VRP	387
10.1.3	Doelen van een VRP	387
10.1.4	Reikwijdte (scope) van een VRP	388

10.1.5	Logische procesfasen van een Verantwoording en Rapportageplan	388
10.1.6	Managementwaarde van een VRP	389
10.1.7	Belang van de FG bij een VRP	389
10.1.8	Behandelplan	389
10.2	VRP: doelen en neveneffecten	390
10.2.1	Algemene doelen van een VRP	390
10.2.1.1	Ex professio rechtstreeks verslag doen	391
10.2.1.2	Inzicht in FG-verwachting: passend gegevensbeschermingsbeleid	392
10.2.1.3	Inzicht in FG-verwachting: passende en effectieve maatregelen	392
10.2.1.4	Inzicht in FG-verwachting: concretisering en naleving van beginselen	392
10.2.1.5	Inzicht in FG-verwachting: rechtmatigheid van verwerkingen	393
10.2.1.6	Inzicht in FG-verwachting: register van verwerkingsactiviteiten	393
10.2.1.7	Inzicht in FG-verwachting: evaluatie en actualisatie	394
10.2.1.8	Inzicht in FG-verwachting: AVG-risk management en control	394
10.2.1.9	Inzicht in FG-verwachting: AVG-issue management	394
10.2.1.10	Inzicht in FG-verwachting: DPIA verplichtingen	395
10.2.2	Neveneffecten van een VRP	395
10.3	AVG-verantwoording en rapportage: processtappen	396
10.3.1	Stap 1: Bepaal het subject van de verantwoordingsrapportage	397
10.3.2	Stap 2: Benoem en benader de stakeholders van de FG-verantwoordingsrapportage	399
10.3.3	Stap 3: Bepaal de scope van de FG-verantwoordingsrapportage	399
10.3.4	Stap 4: Stel een eerste concept samen van de FG-verantwoordingsrapportage	399
10.3.5	Stap 5: Betrek alle AVG-stakeholders	400
10.3.6	Stap 6: Stel de eindversie op van de FG-verantwoordingsrapportage	400
10.4	Verantwoording en rapportage: aandachtspunten voor de FG	400
10.5	Oriëntatietabel FG-werkprogramma: VRP	402
	LITERATUUR	419
	TREFWOORDENREGISTER	423
	BIJLAGEN	439
1.	Algemene verordening gegevensbescherming (AVG), Officiële Nederlandse vertaling, Publicatieblad van de Europese Unie, L119 (04.05.2016).	440
2.	WP 243 rev.01, Richtlijnen voor functionarissen voor gegevensbescherming (Data Protection Officer, DPO), 05 April 2017	528
3.	WP 243 rev.01, Guidelines on Data Protection Officers ('DPOS'), 05 April 2017	559
4.	AEPD, DPO CERTIFICATION SCHEME (SPANJE)	584