1 ALGEMENE BEPALINGEN

Artikel 1 – Begripsbepalingen

Autoriteit Persoonsgegevens (AP)	De Autoriteit Persoonsgegevens, de organisatie die tot taak heeft toe te zien op de Verwerking van Persoonsgegevens conform de geldende wet- en regelgeving.
Betrokkene	Betrokkene(n) in de zin van artikel 4 lid 1 AVG.
Beveiligingsincident	Een inbreuk op de beveiliging of een poging tot een inbreuk of een verstoring van de continuïteit van de Verwerking. Een Beveiligingsincident hoeft niet altijd een Datalek te zijn.
Datalek	Iedere inbreuk in verband met Persoonsgegevens als bedoeld in artikel 33 en 34 van de AVG.
Derde	Ieder ander dan de Betrokkene, de Verwerkings- verantwoordelijke, de gebruiker of de Verwerker.
Dienstenovereenkomst	De overeenkomst tussen Verwerkingsverantwoorde– lijke en Verwerker ter zake van de levering van diensten door C&F B.V., ook wel de hoofd– overeenkomst.
Persoonsgegeven(s)	Persoonsgegeven(s) in de zin van artikel 4 lid 1 AVG.
Subverwerker	Elke navolgende verwerker ingeschakeld door de Verwerker die ermee instemt om Persoonsgegevens te Verwerken namens de Verwerker, ten behoeve van de Verwerkingsverantwoordelijke.
Toestemming van de Betrokkene	Elke vrije, specifieke en op adequate informatie berustende wilsuiting van de Betrokkene waarmee deze aanvaardt dat op hem/haar betrekking hebbende Persoonsgegevens worden verwerkt.
Verstrekken van Persoonsgegevens	Het bekendmaken of ter beschikking stellen van Persoonsgegevens die in de registratie(s) zijn opgenomen of die door Verwerking daarvan, al dan niet in verband met andere gegevens, zijn verkregen.
Verwerker	Verwerker in de zin van artikel 4 lid 8 van de AVG. Dit is C&F B.V., Pedro de Medinalaan 9, 1086 XK Amsterdam.
Verwerkersovereenkomst	Deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.
Verwerking	Verwerking in de zin van artikel 4 lid 2 van de AVG.
Verwerkingsverantwoordelijke	Verwerkingsverantwoordelijke in de zin van artikel 4 lid 7 van de AVG.

Artikel 2 – Toepassingsgebied

Dit reglement is van toepassing op elke al dan niet geautomatiseerde Verwerking van Persoons- gegevens alsmede de niet geautomatiseerde Verwerking van Persoonsgegevens die in de Dienstenovereenkomst zijn opgenomen of die bestemd zijn om daarin opgenomen te worden.

2 KENMERKEN VAN DE VERWERKING VAN PERSOONSGEGEVENS

Artikel 3 – Doel van de gegevensverwerking

De gegevensverzameling wordt in stand gehouden ten behoeve van alle licentiehouders voor het onderhouden van contacten met relaties in het kader van voor die relaties uit te voeren opdrachten.

Artikel 4 – Rechtmatige gegevensverwerking

1. De Verwerkingsverantwoordelijke draagt er zorg voor dat Persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt.

2. De gegevens worden alleen Verwerkt door personen die krachtens een (arbeids)- overeenkomst tot geheimhouding zijn verplicht.

3. Persoonsgegevens worden verwerkt voor de in artikel 3 beschreven doeleinden en worden niet verwerkt indien:
   - Betrokkene voor de Verwerking expliciet zijn toestemming heeft onthouden, of;
   - De gegevensverwerking niet noodzakelijk is voor de uitvoering van de doelstelling van de gegevensverzameling.

4. De Verwerkingsverantwoordelijke bewaart geheimhouding over de Persoonsgegevens waarvan hij/zij kennisneemt, behoudens voor zover enig wettelijk voorschrift hem/haar tot mededeling verplicht of uit zijn/haar taak mededeling voortvloeit.

5. Persoonsgegevens mogen verwerkt worden ten behoeve van wetenschappelijk onderzoek mits dit geanonimiseerd geschiedt.

Artikel 5 – Persoonsgegevens

De navolgende Persoonsgegevens kunnen door de Verwerker met inachtneming van het bepaalde in dit reglement worden verwerkt.
- NAW-gegevens.

Artikel 6 – Toegang tot Persoonsgegevens

De volgende personen hebben toegang tot de gegevens:
- De Verwerkingsverantwoordelijke;
- De Verwerker.

De volgende medewerkers hebben toegang tot Persoonsgegevens:
- Pieter Koenders, Managing Director;
- Marieke van Gemert, projectmanager.

Artikel 7 – Subverwerkers

De volgende Subverwerkers worden ingezet voor de Verwerking van Persoonsgegevens:
- Administratiesysteem SymSys.

3 RECHTEN VAN DE BETROKKENEN

Artikel 7 – Informatieverstrekking aan Betrokkene

1. Indien bij de Betrokkene de Persoonsgegevens worden verkregen, deelt de Verwerkings- verantwoordelijke voor het moment van verkrijging de Betrokkene mede:
   - zijn identiteit;
   - de doeleinden van de verwerking waarvoor de Persoonsgegevens zijn bestemd, tenzij de Betrokkene daarvan reeds op de hoogte is.

2. De Verwerkingsverantwoordelijke verstrekt nadere informatie voor zover dat gelet op de aard van de Persoonsgegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt nodig is om tegenover de Betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.

Artikel 8 – Recht op inzage en afschrift van opgenomen Persoonsgegevens

1. De Betrokkene heeft het recht kennis te nemen van de op zijn persoon betrekking hebbende verwerkte gegevens. De gevraagde inzage en/of het gevraagde afschrift zal zo spoedig mogelijk, doch uiterlijk binnen drie weken na het verzoek worden verstrekt aan de Betrokkene.

2. Afschriften van Persoonsgegevens worden aan de Betrokkene verstrekt tegen de wettelijk vastgestelde kostenvergoedingen.

3. Recht op inzage of afschrift kan worden geweigerd als dit noodzakelijk is in het belang van de bescherming van de persoonlijke levenssfeer van een ander.

Artikel 9 – Recht op afscherming, aanvulling en correctie van opgenomen Persoonsgegevens

1. Desgevraagd worden de opgenomen Persoonsgegevens aangevuld met een door de Betrokkene afgegeven verklaring met betrekking tot de opgenomen Persoonsgegevens.

2. De Betrokkene kan verzoeken om correctie of afscherming van op hem betrekking hebbende Persoonsgegevens indien deze feitelijk onjuist, voor het doel van de Verwerking onvolledig of niet ter zake dienend zijn, dan wel in strijd met een wettelijk voorschrift, in de Verwerking voorkomen.

3. De Verwerkingsverantwoordelijke bericht de verzoeker binnen drie weken na ontvangst van het schriftelijk verzoek tot correctie of aanvulling schriftelijk of, dan wel in hoeverre, hij daaraan voldoet. Een weigering is met redenen omkleed.

Artikel 10 – Recht op vernietiging van opgenomen Persoonsgegevens

1. De Betrokkene kan schriftelijk verzoeken om vernietiging van op hem betrekking hebbende Persoonsgegevens. Indien de bewaring van aanmerkelijk belang is voor een ander dan Betrokkene of indien er een wettelijke plicht tot bewaring van de gegevens geldt, worden de Persoonsgegevens niet vernietigd.

2. De Verwerkingsverantwoordelijke bericht de verzoeker binnen drie weken na ontvangst van het schriftelijk verzoek tot verwijdering of vernietiging schriftelijk of, dan wel in hoeverre, hij daaraan voldoet. Een weigering is met redenen omkleed.

3. De Verwerkingsverantwoordelijke verwijdert of vernietigt de Persoonsgegevens binnen drie maanden na een daartoe strekkend verzoek van de Betrokkene, tenzij redelijkerwijs aannemelijk is dat de bewaring van aanmerkelijk belang is voor een ander dan de Betrokkene, alsmede voor zover bewaring op grond van een wettelijk voorschrift vereist is.

4 BEVEILIGING

Artikel 11 – Beveiliging en afhandelen incidenten en de Meldplicht datalekken

1. De Verwerkingsverantwoordelijke conformeert zich aan de meldplicht datalekken zoals deze in de beleidsregels van de meldplicht zijn beschreven. Dit geschiedt in overleg met de Verwerker volgens het protocol dat de Verwerker heeft opgesteld. De Verwerkings- verantwoordelijke treft maatregelen om de AP en Betrokkenen te informeren indien dit in het kader van de meldplicht aan de orde is.

2. De Verwerkingsverantwoordelijke en de Verwerker treffen passende technische en organisatorische maatregelen om Persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige Verwerking zoals in artikel 4 bedoeld. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de ten uitvoerlegging, een passend beveiligingsniveau, gelet op de risico's die de verwerking en de aard van de te beschermen Persoonsgegevens met zich meebrengen.

PROCEDURE MELDING EN AFHANDELING DATALEK

Inleiding

Dit document beschrijft de verschillende stappen die binnen C&F B.V. worden genomen bij een datalek, dat valt onder de Meldplicht Datalekken. Bij een datalek is sprake van een inbreuk op de beveiliging van persoonsgegevens als bedoeld in artikel 33 en 34 van de AVG.

Datalekken kunnen ontstaan door onder andere:
- moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, malwarebesmetting);
- technisch falen (ICT-storingen);
- menselijk falen (te eenvoudige wachtwoorden/het verstrekken van gebruikersnaam/ wachtwoord aan collega's en/of externen);
- calamiteit (brand datacentrum, wateroverlast);
- verlies van USB-stick of laptop;
- verzenden van e-mailberichten met e-mailadressen van alle geadresseerden in de c.c.;
- het onrechtmatig verwerking van gegevens.

Een datalek moet onverwijld, binnen 24 uur nadat de verantwoordelijke binnen C&F B.V. er kennis van heeft genomen, bij de Verwerkingsverantwoordelijke worden gemeld. De Verwerkingsverantwoordelijke dient binnen 72 uur na ontdekking van het datalek dit te melden aan de Autoriteit Persoonsgegevens.

Het datalek moet, in sommige gevallen, ook worden gemeld bij de betrokkenen. In het geval van C&F B.V. zijn dit over het algemeen klanten (licentiehouders en betrokkenen) of medewerkers. Betrokkenen zijn degenen van wie de persoonsgegevens zijn betrokken bij een inbreuk. De betrokkene moet onverwijld in kennis worden gesteld van de inbreuk, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor zijn persoonlijke levenssfeer.

Een Verwerker (2) is verplicht om een datalek te melden bij de Verwerkingsverantwoordelijke (1).

1. Verwerkingsverantwoordelijke: de Verwerkingsverantwoordelijke heeft zeggenschap over doel en wijze van verwerking. Formeel, juridisch en feitelijk (functioneel) is de Verwerkingsverantwoordelijke degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Hij/zij is degene die zeggenschap heeft over en verantwoordelijk is voor doel en middelen van verwerking en beslist over bewaartermijnen, verstrekking inzageverzoeken etc. De Verwerkingsverantwoordelijke heeft de regierol (regie over het beheer van privacy in de keten).

2. Verwerker: degene die de gegevens ten behoeve van de Verwerkingsverantwoordelijke verwerkt zonder aan zijn of haar rechtstreeks gezag te zijn onderworpen (ook extern). De Verwerker verwerkt persoonsgegevens overeenkomstig de instructies en uiteindelijke verantwoordelijkheid van de Verwerkingsverantwoordelijke. De Verwerker neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens etc.

Melden

Alle datalekken van persoonsgegevens moeten intern worden gemeld en worden gedocumenteerd door de Functionaris Gegevensbescherming (FG). De melding kan door iedere medewerker en iedere Verwerker worden gedaan. De melding kan ook door een extern persoon worden gedaan bij een medewerker van C&F B.V. De melding moet direct en telefonisch worden gedaan bij de FG en schriftelijk worden vastgelegd. De FG meldt het datalek zo nodig bij de Autoriteit Persoonsgegevens (APG). Buiten kantoortijden kan/moet de FG bereikbaar zijn!

De FG legt vast:
- naam van de melder;
- datum en tijd van de melding;
- aard van de inbreuk (is er aanmerkelijk risico op verlies of onrechtmatige verwerking?);
- welke persoonsgegevens vallen onder de melding;
- om welk aantal en/of gegevensrecords gaat het;
- welke (groepen) personen zijn betrokken bij de melding;
- welke maatregelen zijn of worden door de melder getroffen;
- welke gevolgen zijn er volgens de melder voor de betrokkenen;
- de contactpersoon voor de melding.

Eerste analyse

De FG beoordeelt of van de inbreuk 'redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking, waaraan nadelige gevolgen voor de privacy van de betrokkenen zijn verbonden'. Is dit niet het geval, dan vindt alleen registratie van de melding plaats door de FG.

Buiten kantoortijden en in het weekend wordt de melding gedaan bij de FG. Bij het niet kunnen bereiken van de FG wordt de melding gedaan bij de beveiligingsbeheerder (security officer).

Responsteam Datalek

Het Responsteam Datalek wordt met een hoge prioriteit bijeengeroepen door de FG. De bijeenkomst wordt voorgezeten door de FG. Het responsteam bespreekt en legt vast:
- de gegevens die door de FG zijn vastgelegd bij het aannemen van de melding;
- de noodzakelijke vervolgacties met betrekking tot het datalek (lek onmiddellijk dichten, toegang tot informatie beperken en tegelijkertijd meer informatie vergaren over de indringer;
- wat zal worden gemeld bij de APG door de FG (naast aard inbreuk, welke persoonsgegevens, aantal betrokken personen/records):
  - de mogelijke gevolgen voor de betrokkenen;
  - de maatregelen die C&F B.V. neemt en/of kan nemen om de schade voor betrokkenen te verkleinen;
  - de maatregelen die betrokkenen kunnen nemen om verdere schade te verkleinen, inclusief de wijze van inlichten hierover;
  - contactgegevens voor betrokkenen.
- de wijze van afhandeling intern, inclusief communicatie met melder, betreffende afdeling(en) en manager(s);
- of er sprake is van eigen aansprakelijkheid of aansprakelijkheid van derden, zoals uit hoofde van wanprestatie (omdat een geheimhoudingsverplichting is geschonden, of in strijd met een contractuele verplichting onvoldoende beveiliging is gerealiseerd) of onrechtmatige daad;
- het al dan niet doen van aangifte en vaststellen of sprake is van strafrechtelijke verwijtbaarheid. Dit kan bijvoorbeeld spelen wanneer er sprake is van betrokkenheid vanuit C&F B.V. zelf, een Verwerker, of wanneer er onvoldoende maatregelen zijn getroffen om ongeregeldheden te voorkomen. Indien gewenst vindt overleg plaats met een juridisch adviseur;
- wat intern wordt gecommuniceerd en op welk moment;
- wat extern gecommuniceerd wordt en op welk moment; er wordt vastgesteld of de pers geïnformeerd moet worden;
- of naast de APG ook andere stakeholders geïnformeerd dienen te worden;
- of er individuen, bedrijven of andere organisaties geïnformeerd worden;
- op welke wijze er intern wordt gerapporteerd, inclusief actiehouder;
- of eventuele schade is gedekt door de verzekering.

Vervolg

De FG rapporteert aan de directie van C&F B.V. de uitkomsten van het overleg van het Responsteam Datalek. De directie van C&F B.V. accordeert de uit te voeren activiteiten, zoals vastgesteld door het Responsteam Datalek of stelt de uit te voeren activiteiten bij. De door de directie van C&F B.V. vastgestelde activiteiten worden uitgevoerd.

Melding bij de APG (Autoriteit Persoonsgegevens)

De FG meldt binnen twee dagen volgens de aangewezen methode het datalek bij de APG. In ieder geval zal moeten worden gemeld:
- aard van de inbreuk, waaronder betrokken categorieën, aantal betrokkenen, aantal gegevensrecords;
- beschrijving van de te verwachten gevolgen;
- getroffen en/of voorgestelde maatregelen;
- informatie over te nemen maatregelen door de betrokkene om de nadelige gevolgen te beperken;
- contactgegevens van betrokkene.

Afwezigheid FG

Bij afwezigheid van de FG wordt diens rol ingevuld door de Managing Director, Pieter Koenders.

MODEL MELDINGSFORMULIER

Op _____ is door _____ geconstateerd dat zich een beveiligingsincident heeft voorgedaan ter zake van de database/applicatie die wordt gehost op _____ te _____

Het incident heeft betrekking op _____ (beschrijving applicatie) waarin de navolgende data zijn opgenomen. De navolgende persoonlijke data zijn mogelijk gecompromitteerd:

_____
_____
_____
_____

(Hierbij dient de aard van de gegevens te worden benoemd: met name bijzondere gegevens of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties.)

De verantwoordelijk(en) is/zijn op _____ (datum) geïnformeerd over het incident.
De navolgende beveiligingsmaatregelen zijn genomen om verdere verspreiding van data te voorkomen en de database op een hoger niveau te beveiligen.

_____
_____
_____
_____

Partijen hebben een incidentresponsteam geformeerd waarin de navolgende personen namens partijen zitting hebben. Het incidentresponsteam opereert onder verantwoordelijkheid van de daartoe aangewezen verantwoordelijke die tevens de communicatie met de Autoriteit Persoonsgegevens verzorgt.

_____
_____
_____
_____

_____ (naam)
_____ (telefoonnummer)
is aangewezen om nadere informatie te verstrekken over het datalek.

PRIVACY-IMPACT-ASSESSMENT

1. Persoonsgegevens
Welke persoonsgegevens worden er allemaal verwerkt? Er zijn twee typen persoonsgegevens: gewone gegevens en bijzondere gegevens. Dit laatste type informatie is gevoelige informatie, bijvoorbeeld hobby's, geloofsovertuiging of zelfs geslacht.
Gewoon: NAW-gegevens.
Bijzonder: niet van toepassing.

2. Gegevensverwerkingen
Wat zijn de verschillende kanalen waarin gegevens worden verwerkt?
- Administratiesysteem SymSys.
- Excel-programma.

3. Verwerkingsdoelen
Wat is het doel van deze gegevenswerkingen?
1. Bijhouden van zakelijke relaties en hun contactgegevens.
2. Versturen van nieuwsbrieven naar mensen die zich daarvoor hebben aangemeld.

5. Belangen bij de gegevensverwerkingen
Wat is het belang van de gegevenswerkingen? Actueel houden van de relevante NAW-gegevens.

6. Verwerkingslocaties
In welke landen worden gegevens verwerkt? Nederland.

7. Technieken en methoden van de gegevensverwerkingen
Met welke technieken, middelen en methoden worden de gegevens verwerkt? Geef hierbij aan of het een geautomatiseerd is handmatig proces is.
- Administratiesysteem SymSys, handmatig.
- Excel-programma, handmatig.

8. Bewaartermijnen
Gedurende welke termijn blijven persoonsgegevens opgeslagen? En waarom worden deze termijnen gehanteerd?
Doorlopend, is kern van de onderneming.

9. Rechtsgrond
Wat is de wettelijke rechtvaardiging van het verwerken van de gegevens? Hebben betrokkenen bijvoorbeeld toestemming gegeven?
- Klantrelatie: klant tekent offerte voor akkoord of geeft hierop per e-mail akkoord.
- Acquisitiedoeleinden.

10. Doelveranderingen
Worden gegevens nog altijd verwerkt conform de oorspronkelijke doelen? Of zijn deze veranderd? Zo ja: passen de huidige doelen nog bij de oorspronkelijke?
Niet van toepassing; elk jaar en ook periodiek wordt dit bijgehouden.

11. Proportie
Zijn de gegevens die verwerkt worden proportioneel met de doelen van de verwerking? Of wordt meer informatie verwerkt dan nodig is?
Verwerkte gegevens zijn proportioneel met de doelen van verwerking. Er wordt niet meer informatie verwerkt dan nodig is.

12. Rechten van de betrokkenen
Welke rechten hebben betrokkenen na de verwerking van hun gegevens? En zijn deze duidelijk gecommuniceerd?
Niet gecommuniceerd, is common practice.

13. Risico's
Wat zijn de risico's van de gegevensverwerkingen?
1. Wat zijn de negatieve gevolgen die gegevensverwerkingen kunnen hebben voor de betrokkenen?
   Geen.
2. Wat is de oorsprong van deze gevolgen?
   Niet van toepassing.
3. Wat is de waarschijnlijkheid dat het mis gaat?
   Gaat niet mis, met uitzondering van de mogelijkheid van datalekken.
   Dan treedt de procedure datalekken in werking.
4. Wat is de ernst van deze gevolgen voor de betrokkenen wanneer het fout gaat?
   Geen, het betreft alleen openbare NAW-gegevens.

14. Maatregelen
Welke technische, organisatorische en juridische maatregelen zijn of worden genomen om de hierboven beschreven risico's te voorkomen of te verminderen? Beschrijf hierbij welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Als een maatregel het risico verhelpt, motiveer dan waarom het restrisico acceptabel is.
Formeel/administratief: Er worden alleen NAW-gegevens opgeslagen. Andere informatie is niet relevant voor C&F B.V.
Gedrag: Data worden nauwkeurig bijgehouden.
Technisch: I-cloudtoepassing is mede, gegeven de datagevoeligheid van de werkzaamheden van C&F B.V.,(deels koersgevoelige informatie) triple-secured beveiligd. Geprinte data worden gecertificeerd vernietigd door de firma Brantjes.

PRIVACYBIJSLUITER BIJ VERWERKERSOVEREENKOMST

A. Algemene informatie
Naam verwerker: C&F B.V.

Beknopte uitleg en werking product
C&F B.V. richt zich bij zijn bedrijfsactiviteiten met name op het produceren en realiseren van corporate, financiële en aanverwante uitingen, zowel in print als online, voor de profit- en not-for-profitsector. In de betreffende dienstverlening kan het voorkomen dat persoonsgegevens van relaties, dan wel indirect betrokkenen, worden verwerkt en/of opgeslagen in systemen en databases.

Verantwoordelijke aan de zijde van verwerker is het management van C&F B.V., zijnde de Managing Director, Pieter Koenders.

B. De specifieke diensten
Consultancy en design. Er worden alleen NAW-gegevens verwerkt. Alle andere informatie wordt niet bijgehouden of verwerkt.

C. Doeleinden en middelen voor het verwerken van gegevens
De verwerker is leverancier van de applicatie en stelt de applicatie ter beschikking aan zijn relatie, als zijnde verwerkingsverantwoordelijke.

D. Categorieën en soorten persoonsgegevens
In het kader van de verwerking worden de volgende (categorieën van) persoonsgegevens verwerkt:
- NAW-gegevens.

E. Algemene informatie over getroffen beveiligingsmaatregelen
Voor de genomen veiligheidsmaatregelen wordt kortheidshalve verwezen naar bijlage 2 bij de verwerkersovereenkomst.
Specifieke beveiligingsmaatregelen voor deze dienst/product: beveiligde toegang en versleutelde opslag.
Eventuele certificeringen: niet van toepassing.
Audits/derden-verklaringen: niet van toepassing.
Plaats/Land van opslag en Verwerking van de Persoonsgegevens: Nederland.

F. Contactgegevens
Voor vragen of opmerkingen over deze bijsluiter kunt u terecht bij onze functionaris gegevensbescherming, Pieter Koenders, p.koenders@cfreport.nl.

Voor opmerkingen over de werking van de applicatie kunt contact opnemen met uw vaste contactpersoon.

VERWERKINGSREGISTER

Type gegevens	Wettelijke basis	Veiligheidsmaatregelen	Ja /Nee
a. Identificatiegegevens	Toestemming	Informatieveiligheidsbeleid	Ja
b. Financiële bijzonderheden	Contractuele overeenkomst	Risico-analyse en veiligheidsplan	Ja
c. Persoonlijke kenmerken	Wettelijke verplichting	Aanstelling van een DPO / VC	Ja
d. Fysieke gegevens	Vitaal belang	Organisatie van informatieveiligheid	Ja
e. Leefgewoonten	Taak van algemeen belang	Medewerkersgerelateerde veiligheid	Neen
f. Psychische gegevens	Gerechtvaardigd belang	Asset Management	Neen
g. Samenstelling van het gezin		Toegangscontrole (logisch)	Neen
h. Vrijetijdsbesteding en interessen		Cryptografie	Neen
i. Lidmaatschappen		Fysieke beveiliging	Neen
j. Gerechtelijke gegevens betreffende ...		Operationele veiligheid	Neen
k. Consumptiegewoonten		Communicatiebeveiliging	Neen
l. Woningkenmerken		System acquisition, development and maintenance	Neen
m. Gegevens betreffende de gezondheid		Leveranciers- en verwerkersrelaties	Neen
n. Opleiding en vorming		Veiligheidsincident- en datalekmanagement	Neen
o. Beroep en betrekking		Business Continuity Management	Neen
p. Rijksregisternummer / Identificatienummer van de sociale zekerheid		Compliance & Verantwoording	Neen
q. Raciale of etnische gegevens			Neen
r. Gegevens over het seksuele leven			Neen
s. Politieke opvattingen			Neen
t. Lidmaatschap van een vakvereniging			Neen
u. Filosofische of religieuze overtuigingen			Neen
v. Beeldopnamen			Neen
w. Geluidsopnamen			Neen
x. Genetische gegevens			Neen
y. Biometrische gegevens			Neen
z. Locatiegegevens			Neen