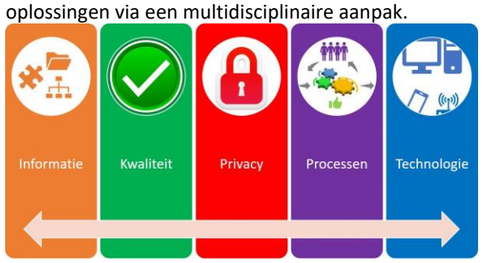
Deze AVG mini gids wordt u aangeboden door Cofian Privacy & Management Consulting B.V.

Cofian houdt zich bezig met het vertalen van organisatorische vraagstukken naar praktische oplossingen via een multidisciplinaire aanpak.



Informatie-, organisatie en procesmanagement wordt gecombineerd met brede en diepgaande kennis van kwaliteit, privacy & security en informatietechnologie.

Cofian is gevestigd in Emmen en werkzaam in heel Nederland. Wij kunnen Europees opereren en er is ruime ervaring met multinationaal opererende ondernemingen, het MKB, ZZP en andere organisaties.

Voor de dienstverlening wordt geen onderscheid gemaakt in de branche of omvang van een organisatie.

Cofian ziet privacy als kernwaarde voor organisatie en individu. Daarom is naast de zakelijke dienstverlening het geven van voorlichting over privacy voor Cofian een zeer belangrijk sociaalmaatschappelijk speerpunt.

cofian
privacy & management consulting

mini AVG gids

Algemene Verordening Gegevensbescherming

(EU General Data Protection Regulation)

Messenger-code

Contactinfo QR code

Cofian Privacy & Management Consulting BV
Marco Polostraat 16 | 7825 VM Emmen
KvK Emmen 67833411 | BTW NL857191378B01 | IBAN NL28KNAB0255750765

0591 - 238093
www.cofian.nl
info@cofian.nl

volg Cofian via

LinkedIn

facebook

Vanaf 25 mei 2018 geldt de AVG Algemene Verordening Gegevensbescherming

De AVG is de Europese wet (EU / GDPR – General Data Protection Regulation) die in Nederland de plek van de Wet bescherming persoonsgegevens zal innemen.

De AVG is op 24 mei 2016 in werking getreden en wordt 25 mei 2018 van kracht. Organisaties hebben twee jaar de tijd om compliant te worden aan de AVG.

Met de nieuwe aangescherpte wetgeving verdwijnt elke vorm van vrijblijvendheid met betrekking tot de bescherming van privacy en informatiebeveiliging. Organisaties moeten nu aantonen compliant te zijn aan deze wetgeving. De aansprakelijkheid ligt bij directie en management en is niet overdraagbaar.

De maatregelen en acties die een organisatie moet nemen voor de AVG zijn sterk afhankelijk van de werkzaamheden, soort en omvang van de organisatie en de huidige stand van zaken binnen een organisatie.

Informatiebeveiliging gaat over bedrijfscontinuïteit en is een taak van directie en management. Correcte implementatie en controle op compliance is maatwerk en vraagt specialistische kennis en ervaring.

Deze minigids is verre van allesomvattend. Het is een wegwijzer die de belangrijkste punten kort samenvat en richting probeert te geven aan wat moet gebeuren.

1. PRIVACY EN AVG: GEEN (IT) HYPE!

Privéleven is een fundamenteel recht en vastgelegd in de **"UN Universal Declaration of Human Rights"** en de **"the International Covenant on Civil and Political Rights"**.

Dit geeft ons onder andere stemrecht, gewetensvrijheid en vrijheid van meningsuiting, maar ook het recht privé echt privé te laten zijn zodat we kunnen zijn wie we zijn.

In de moderne tijd van mondialisering, globalisering en digitalisering zijn Privacy en wetgeving zeker geen hype!

Historie Nederlandse wetgeving gegevensbescherming:
1989: Wet persoonsregistratie (Wpr)
- Toezichthouder: de Registratiekamer

2001: Wet bescherming persoonsgegevens (Wbp)
- Toezichthouder: College bescherming persoonsgegevens
2016: Toevoeging meldplicht datalekken aan de Wbp
- Toezichthouder: Autoriteit Persoonsgegevens (AP)

2018: Algemene verordening gegevensbescherming
- Toezichthouder: Autoriteit Persoonsgegevens (AP)

De AVG is een vervolgstap in verantwoordelijk omgaan met persoonsgegevens met meer controle en toezicht.

2. VOOR WIE GELDT DE AVG

De AVG geldt voor publieke en private organisaties in de EU die als gevolg van hun activiteiten persoonsgegevens verwerken van betrokkenen (ongeacht hun woon- of verblijfplaats) en voor publieke en private organisaties buiten de EU indien zij persoonsgegevens verwerken van betrokkenen in de EU.

- **Overheid**
- **Ondernemingen (profit en non-profit)**
- **Stichtingen**
- **Verenigingen**

'… dus ook voor ZZP-ondernemers, zorginstellingen, sportvereniging en liefdadigheidsstichtingen …'

Materieel toepassingsgebied
De AVG is van toepassing op verwerking van persoonsgegevens in het kader van de activiteiten van een in de EU gevestigde organisatie. De AVG geldt voor zowel de verantwoordelijke (**controller**) als de verwerker **(processor)** van die gegevens, ongeacht plaats van verwerking (binnen of buiten de EU).

Territoriaal toepassingsgebied
Naast de EU is de AVG ook van toepassing op organisaties buiten de EU als die organisaties persoonsgegevens verwerken van personen die zich in de EU bevinden en die verwerking verband houdt met het aanbieden van diensten en/of goederen of monitoring van persoonsgedrag binnen de EU.

3. WAT ZIJN PERSOONSGEGEVENS

Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijk persoon.

Dat betekent dat elk gegeven wat direct of indirect leidt naar of gelinkt kan worden aan een natuurlijk persoon moet worden gezien als een persoonsgegeven.

Een greep uit het assortiment persoonsgegevens:

- **Naam, adres en woonplaats**
- **Telefoonnummer**
- **IP-nummer**
- **Registratienummers zoals het BSN-nummer**
- **Ras**
- **Sekse**
- **E-mail**
- **Geloofsovertuiging**
- **Medische gegevens**
- **(Geestelijke) gezondheid**
- **Financiële gegevens**
- **Strafrechtelijk verleden**

Persoonsgegevens zijn bijvoorbeeld ook:

- **Foto's van personen of persoonsgegevens**
- **Opgeslagen video zoals camerabewaking**
- **Opgeslagen audio zoals telefoongesprekken**

4. ENKELE DEFINITIES UIT DE AVG

ANONIMISERING	•Verwijderen van persoonsgegevens
BETROKKENE	•Eigenaar van persoonsgegevens, EU-burger
DATA PROTECTION IMPACT ASSESSMENT	•DPIA; risico analyse omtrent gegevensbescherming
ENCRYPTIE	•Het coderen van email en/of bestand door een algoritme
FUNCTIONARIS GEGEVENSBESCHERMING	•Verantwoordelijke voor naleving en bewaking AVG
PERSOONSGEGEVEN	•Gegeven van identificeerbaar of geïdentificeerde persoon
DATA PROTECTION BY DEFAULT	•Applicatie instellingen dienen privacyvriendelijk te zijn
DATA PROTECTION BY DESIGN	•Bij ontwikkeling van applicatie rekening houden met security
PRIVACY IMPACT ASSESSMENT (PIA)	•Risico analyse omtrent privacy / persoonsgegevens
PSEUDONIMISERING	•Het vervangen of scheiden van persoonsgegevens
VERANTWOORDELIJKE (controller)	•Wie het doel en de wijze van gegevensverwerking bepaald
VERWERKER (processor)	•Derde die gegevens verwerkt (opdracht verantwoordelijke)

5. INVENTARISATIE

1. • Inventariseer huidige situatie (0-meting)
   • Inkaderen organisatiestructuur & AVG
2. • Breng alle persoonsgegevens in kaart
   • Breng alle informatiestromen in kaart
3. • Toets wettelijke grondslag van gegevens
   • Toets huidige contracten en statements
4. • Controleer classificatie van gegevens
   • Controleer procedures en instructies
5. • Toets kennisniveau AVG
   • Toets communicatieniveau AVG
6. • Samenstellen werkgroep & key-users
   • Rapportage en bespreking 0-meting
7. • Opstellen bewustwordingstraject
   • Opstellen plan van aanpak AVG traject

6. BASISBEGINSELEN

WETTELIJKE GRONDSLAG VERWERKING PERSOONSGEGEVENS
VASTLEGGEN | TOESTEMMING

TRANSPARANTIE MET BETREKKING TOT VERWERKING
HOE | WAT| WAAROM | WAAR | HELDER EN BEGRIJPELIJK

VASTLEGGING RECHTEN EN PROCEDURES
VERANTWOORDELIJKE | BETROKKENE

BEVEILIGING UITGANGSPUNT BIJ IT-MIDDELEN / APPLICATIES
DATA PROTECTION BY DESIGN | DATA PROTECTION BY DEFAULT

OVEREENKOMSTEN EN VERKLARINGEN
VERWERKERSOVEREENKOMST | PRIVACY STATEMENT

DATALEKKEN
PROCEDURES | (IT) BEVEILIGINSMIDDELEN

COMPLIANCE
DATA PROTECTION OFFICER | PRIVACY IMPACT ASSESSMENT

7. PROCEDURES EN VASTLEGGING

De AVG, een document van 84 bladzijden, is verdeeld over 173 overwegingen en 99 artikelen een veel uitgebreidere wetgeving dan de huidige Wbp. De AVG is te omvangrijk voor deze gids maar enkele **punten van aandacht:**

ZORGPLICHT INFORMATIEBEVEILIGING
- AVG kan directie en/of management aansprakelijk stellen
- Geen verlegging aansprakelijkheid naar betrokkene(n)
- Opstellen beleid voor privacy en informatiebeveiliging

VERWERKINGSREGISTER
- Vastleggen hoe privacy gegevens worden verwerkt, dit register moet alle verwerkingsactiviteiten bevatten
- Verplicht voor zowel de processor (verwerker) als de controller (verantwoordelijke)

CLASSIFICATIE VAN PERSOONSGEGEVENS
- Classificatie van gegevens, doel en bewaartermijnen

PROCEDURE MELDPLICHT DATALEKKEN
- Hoe te handelen bij datalekken of beveiligingsincidenten
- Opstellen en bijhouden incidenten- en verwerkersregister

PROCEDURES VOOR RECHTEN & PLICHTEN BETROKKENEN
- Alle rechten en plichten van betrokkenen moeten in aparte procedures worden vastgelegd en beschikbaar gesteld. Inclusief maar niet beperkt tot vergeetrecht, correctierecht, recht op inzage en recht op dataportatie

8. HULPMIDDELEN (IT)

Informatiebeveiliging is een verantwoording voor directie en management, niet van de IT. Informatietechnologie is een hulpmiddel, geen doel op zich.


FIREWALL: reguleer, controleer en beveilig dataverkeer


ENCRYPTIE: encrypt bestanden en email (is eenvoudiger en minder belastend dan het lijkt)


BACKUP: zorg voor een goede backup en test deze regelmatig


DISASTER RECOVERY PLAN: bedrijfszekerheid en continuïteit

IAM Identity Access Management: beveilig, monitor en controleer

Toegangsbeveiliging: biometrie, token, 2weg-authenticatie, etc.

9. DATALEKKEN

Bij een datalek is sprake van inbreuk op de integriteit, vertrouwelijkheid en beschikbaarheid van persoonsgegevens. Een situatie waarbij onrechtmatig gebruik niet kan worden uitgesloten is ook een datalek.

Een basis leidraad

BEVEILIGINGSINCIDENT
- Classificeren
- Registreren

→ **ANALYSE datalek ja/nee**
- Risico
- Impact

↓

PERSOONSGEGEVENS GELEKT / VERLOREN*?
- JA: Datalek, melden binnen 72 uur aan AP
- NEE: Geen Datalek

→ **ENCRYPTIE GEBRUIKT?**
- JA: Inlichten betrokkene waarschijnlijk niet nodig**
- NEE: Melden aan betrokkenen**

↓

NADELIGE GEVOLGEN VOOR BETROKKENEN?
- JA: Melden aan betrokkenen**
- NEE: Melden afhankelijk van situatie

Het melden moet volgens procedures en voorwaarden
Vraag bij twijfel altijd advies!

De interpretatie van deze leidraad is, vooral waar het gaat om risico en impact, lastig. De functionaris gegevensbescherming adviseert hierin maar de verantwoordelijke blijft eindbeslisser.

10. OVEREENKOMSTEN EN VERKLARINGEN

Overeenkomsten en (privacy)verklaringen zullen moeten voldoen aan de eisen van de AVG om juridisch te kloppen. De vrijblijvendheid binnen overeenkomsten zal vervallen.

VERWERKERSOVEREENKOMST:
In deze verplichte overeenkomst (onder de Wbp bekend als bewerkersovereenkomst) tussen de verantwoordelijke en de verwerker moeten in ieder geval onderstaande punten staan:
- doel van gegevensverwerking & soort persoonsgegeven
- categorieën van betrokkenen & identificatie van rechten
- passende beveiliging & voorwaarden voor audit
- na afloop vernietigen of teruggeven van de gegevens
- toestemming bij inschakelen derden door verwerker
- bewaartermijnen, meldplichtprocedure

Verwerken moet ruim worden geïnterpreteerd. Bij het alleen kunnen inzien van gegevens is er al sprake van verwerking!

DATATRANSFER PERSOONSGEGEVENS BUITEN DE EU
Voor datatransfer van persoonsgegevens naar landen buiten de EU moet een overeenkomst worden opgesteld met de betreffende verwerker buiten de EU (Europees Modelcontract).

PRIVACY STATEMENT:
Deze is verplicht bij verwerking van persoonsgegevens. Gebeurt dit verzamelen van informatie ook via een website, bijvoorbeeld met een contactformulier, dan moet het privacy statement tevens op de website duidelijk zichtbaar worden gepubliceerd.

11. COMPLIANCE

…"compliance begint bij bewustwording"…

Functionaris gegevensbescherming / DPO
De aanstelling van een functionaris gegevensbescherming (FG) is afhankelijk van het soort gegeven en de aard van verwerking. Een FG mag intern worden benoemd. In dat geval heeft de FG ontslagbescherming. De FG mag ook een extern iemand zijn of vanuit een brancheorganisatie worden gefaciliteerd.

Een FG wordt aangemeld bij de Autoriteit Persoonsgegevens en vermeld in het openbare register. De FG is de liaison tussen de toezichthouder en de organisatie en heeft een wettelijk omschreven takenpakket. Bij organisaties die een FG hebben aangesteld communiceert de organisatie met de FG en niet met de autoriteit; de toezichthouder stelt zich dan terughoudend op.

PIA (Privacy Impact Assessment)
Als de verwerking van persoonsgegevens grote risico's inhoudt is het uitvoeren van een PIA verplicht. Een PIA is in ieder geval verplicht bij overheidsinstellingen, grootschalige verwerking van bijzondere persoonsgegevens en implementatie van nieuwe technologie waarmee persoonsgegevens worden verwerkt.

Audit
Organisaties moeten compliance aan de AVG aantoonbaar maken. Daarom moet naast een PIA ook controle zijn die beleid en IT-systemen toetst aan gestelde normen en eisen.

12. CHECKLIST

Checklist met belangrijkste punten

- ☐ Kennis van de AVG
- ☐ Privacybeleid
- ☐ Inkaderen gegevens
- ☐ Verwerkingsregister
- ☐ Toestemmingen
- ☐ Verwerkersovereenkomst
- ☐ Privacy statement
- ☐ Dataportabiliteit
- ☐ Procedures betrokkenen
- ☐ Procedure datalekken
- ☐ EU-US Privacy-Shield contract(en)
- ☐ Functionaris Gegevensbescherming
- ☐ Firewall bescherming
- ☐ Privacy Impact Assessment(s)
- ☐ Toepassing Encryptie
- ☐ Back-up (gevalideerd)
- ☐ Disaster Recovery Plan
- ☐ Toegangsbeveiliging
- ☐ Identiteit management
- ☐ Audit IT-systemen
- ☐ Audit organisatie
- ☐ EU modelcontracten voor data doorgifte buiten EU

Bronnen:
www.autoriteitpersoonsgegevens.nl
www.cofian.nl