



# WHITEPAPER

PRAKTISCHE HANDREIKING VOOR DE ALGEMENE VERORDENING  
GEGEVENSBECHERMING (AVG)

**Hoewel het nog een jaar duurt, is er geen ontkomen meer aan: de Europese privacyverordening gaat ook u raken en werk opleveren. Gelukkig is er nog tijd genoeg om aan de slag te gaan. Guardian360 helpt u hier graag bij. Daarom geven we u in deze whitepaper een helder overzicht van wat u te wachten staat.**

### **WAT IS DE AVG?**

De Algemene Verordening Gegevensbescherming (AVG) is hetzelfde als de General Data Protection Regulation (GDPR). De individuele lidstaten moeten werken met deze nieuwe EU-regulering. De AVG gaat op 25 mei 2018 in en vervangt onze huidige Wet Bescherming Persoonsgegevens (Wbp).

### **WAT STAAT ER IN DE AVG?**

De AVG zorgt voor dezelfde regels omtrent bescherming van persoonsgegevens in heel Europa. Het maakt dan niet meer uit in welk EU-land de burger, wiens gegevens worden verwerkt, woont; het gaat om 'betrokkenen die zich in de Unie bevinden'.

Er zullen meer verplichtingen gaan gelden dan bij de Wbp en de Meldplicht Datalekken – die u hopelijk al kent. Een groot deel van de AVG is echter best praktisch te noemen. Een nadeel is de enorme boete die mogelijk wordt uitgedeeld wanneer u niet voldoet aan de AVG. Deze boete kan bij zeer ernstige overtredingen oplopen tot maximaal EUR 20 miljoen of 4% van uw wereldwijde omzet.

**GUARDIAN**  **360°**

### **KORTOM, HIER KOMT HET OP NEER:**

1. U moet exact weten welke bestanden met persoonsgegevens u beheert en in bezit heeft. U moet ook van elk aspect van de persoonsgegevens afzonderlijk kunnen aangeven waarom u deze gegevens opslaat.
2. U moet weten welke rechten de personen hebben van wie u gegevens in bezit heeft.
3. Wanneer u een product of dienst ontwikkelt, dan moet er 'security by design' worden toegepast. U moet dus direct nadenken over hoe u de beveiliging van gegevens waarborgt en inbouwt.
4. Projecten met een hoog risico op lekken moeten vooraf een inschatting van privacy risico's krijgen, een zogenaamde Privacy Impact Analyse (PIA).
5. U mag persoonsgegevens alleen maar gebruiken voor het doel waar de informatie oorspronkelijk voor verzameld is. Ook moet er een 'juridische grondslag' zijn.



**AUTORITEIT  
PERSOONSGEGEVENS**

## WIE DOET WAT?

Uw Guardian360 partner is - wanneer zij data voor u beheren, opslaan, transporteren of verwerken - de zogenaamde processor. U bent als eigenaar van de gegevens de controller. De datacentra die uw Guardian360 partner inzetten om haar servers (waarop weer uw gegevens staan) in te plaatsen, is vaak de sub processor.

U bent als controller verantwoordelijk voor:

1. Het verzamelen van de gegevens en het toestemming hebben of verkrijgen hiervan van de persoon van wie de gegevens zijn.
2. Het zorgen dat deze gegevens alleen voor het doel worden verwerkt waarvoor ze zijn verkregen, en dat ze adequaat worden beveiligd.
3. Het verwijderen van data op verzoek van de persoon van wie de data is.
4. Het aangeven aan Intermax welk niveau van beveiliging vereist is. Uiteraard kunnen we u hierbij helpen.

Uw Guardian360 partner is als processor verantwoordelijk voor:

1. Het fysiek opslaan van de gegevens en de bewaking ervan, zodat er geen onrechtmatige toegang door derden plaatsvindt.
2. Het zorgen dat ook sub processoren (bijvoorbeeld een datacentrum) hieraan voldoet.
3. U te informeren als er afwijkingen of privacy-incidenten zijn.
4. Het beoordelen en afhandelen van vorderingen en taps door bevoegde overheidsinstanties (bijvoorbeeld politie, justitie, AIVD, MIVD).



## OVER DE CYBERRISICO VERZEKERING:

Guardian360 heeft een handige toolkit die u helpt informatie te verzamelen die belangrijk is bij het afsluiten van een Cyber Risico Verzekering. Onderwerpen die hierbij in kaart dienen te worden gebracht, zijn:

1. Assessment: wat heeft u aan middelen en informatie?
2. Incident Response Plan: wat gebeurt er indien een incident optreedt, wie doet wat?
3. Cyber Exposure Data Scheme: welke informatie heeft het grootste gevaar op datalekken in zich?

Met deze informatie kan worden ingeschat welke risico's u loopt en hoe hoog (of hoe laag) uw verzekeringspremie gaat zijn.

### Meer informatie over de Cyberrisico verzekering?

<https://www.guardian360.nl/oplossingen/cyberisico-verzekering/>

Ook moet de verantwoordelijke voor de gegevens toestemming vragen aan de eigenaar van de gegevens wanneer hij onderaannemers inschakelt (voor zover deze persoonsgegevens verwerkt). Dat geldt dus ook wanneer u een derde inschakelt om uw gegevens te beheren en te bewaken.

Overigens moeten bedrijven die buiten de EU zijn gevestigd of die buiten de EU gegevens van Europese burgers verwerken (denk aan Google, Amazon of Microsoft) zich ook aan de AVG houden.

## **WAAR KUNT HET BESTE BEGINNEN?**

Het eenvoudigst is om te beginnen met een inventarisatie van de gegevens die u heeft. U dient dus een antwoord te formuleren op de volgende vragen:

- Welke typen persoonsgegevens worden er binnen onze organisatie verwerkt?
- Wat is het doel hiervan?
- Van welke betrokkenen verwerken wij eigenlijk persoonsgegevens? Om wie gaat het eigenlijk?
- Hoe lang bewaren wij deze gegevens?

Met een overzicht van de antwoorden op deze vragen is het maken van een PIA veel eenvoudiger. Ook kunt u makkelijker klanten te woord staan wanneer ze u vragen naar hun gegevens.

## **WAT TE DOEN ALS HET TOCH FOUT GAAT?**

Het allerbelangrijkste is dat u zo snel als mogelijk contact opneemt met uw Guardian360 partner wanneer u een informatiebeveiligingsincident vermoedt of heeft vastgesteld. De security specialisten zullen dan het bewijs hiervan vastleggen en dit onveranderbaar veilig stellen voor verder forensisch onderzoek. Dat doen zij in veel gevallen proactief wanneer u (een deel van) de informatiebeveiliging heeft uitbesteed aan hen. Wanneer u onze Cyberrisico Verzekering heeft afgesloten, dan zullen wij samen met uw Guardian360 partner actie ondernemen en de verzekeraar inschakelen.



## WAAR MOET U NOG MEER REKENING MEE HOUDEN?

De AVG voorziet in een aantal belangrijke aspecten die niet vergeten mogen worden:

1. Alle betrokkenen hebben uitgebreide rechten:
  - a. Zij mogen gegevens corrigeren als de verzamelde persoonsgegevens onjuist blijken te zijn (artikel 16).
  - b. Zij hebben ook het recht om 'vergeten te worden'; op verzoek dient u gegevens zo spoedig mogelijk ('zonder onredelijke vertraging') te wissen (artikel 17).
  - c. Zij hebben ook het recht om de eigen gegevens in een gestandaardiseerd formaat te ontvangen. Dan is het eenvoudiger om gegevens door te geven aan een andere leverancier van een vergelijkbare dienst, bijvoorbeeld wanneer zij overstappen (artikel 20).
  - d. En uiteraard hebben zij het recht om de eigen gegevens in te zien (artikel 15).
2. U heeft ook een Registerplicht (artikel 30). Dat betekent dat u schriftelijk de belangrijkste aspecten van de persoonsgegevens die u verwerkt, moet vastleggen. Het goede nieuws is dat dit niet geldt voor organisaties met minder dan 250 medewerkers, tenzij:
  - a. U stelselmatig en op grote schaal (bijzondere) persoonsgegevens verwerkt.
  - b. De gegevensverwerking een groot risico voor de betrokkenen inhoudt.

## WAAR MOET U NOG MEER REKENING MEE HOUDEN?

3. U heeft nog steeds een meldplicht bij datalekken, net als in de huidige Wbp, maar:
  1. De drempel wanneer u moet melden is lager geworden. U dient nu elk datalek te melden, mits er geen enkel risico is voor de 'vrijheden en rechten van individuen' (artikel 33).
  2. Het datalek moet gemeld worden 'zonder onnodige vertraging' en binnen 72 uur nadat u deze heeft geconstateerd.
  3. Bij een hoog risico voor de rechten en vrijheden van individuen moet u ook alle betrokkenen op de hoogte stellen (art. 34). Wat 'hoog' is dient u zelf in te schatten.
4. Wanneer u overheidsinstantie bent of een bedrijf dat het observeren van personen als (kern)activiteit heeft, dan moet u een Functionaris Gegevensbescherming (FG) aanstellen (ook wel 'Data Protection Officer' genoemd). Dit geldt ook wanneer u grote hoeveelheden gegevens verzamelt.
5. Maar pas op: kiest u ervoor een FG aan te stellen, dan kunt u niet meer terug indien dit toch niet noodzakelijk bleek. U kunt dit voorkomen door een intern memorandum op te stellen (ondertekend door de directie) waarin u beschrijft waarom u geen FG heeft aangewezen en welke overwegingen u hierbij heeft gehad.



## WAAR EN HOE KUNNEN GUARDIAN360 PARTNERS U HELPEN OM TE VOLDOEN AAN DE AVG?

Een aantal Guardian360 partners levert haar diensten volgens het 'Privacy by Design' principe. Daarmee bedoelen we dat de bescherming van persoonsgegevens, privacy en beveiliging van data in algemene zin zit 'ingebakken' binnen de organisaties en hun werknemers. Vervolgens controleren we dat 24 uur per dag, onder andere met ons Guardian360 security platform. Wanneer u uw persoonsgegevens bij deze Guardian360 partners onderbrengt, kunnen zij daarmee aantonen dat zij al het redelijke doen en hebben gedaan om deze gegevens te beschermen. Aanvullend hierop nemen zij maatregelen om datalekken proactief te voorkomen.

Mocht er onverhoopt toch iets lekken, dan kunt u op basis van het Guardian360 platform aantonen dat u alles hebt gedaan (wat betreft de omgeving die binnen onze scan scope valt) om dit te voorkomen. De kans dat u een boete krijgt, wordt daardoor heel klein.

Ook wanneer u volgens de AVG een Functionaris Gegevensbeheer (FG) dient te hebben, helpen Guardian360 partners u graag. Zij kunnen u helpen een rechtsgeldig document op te (laten) stellen, waarin zij uiteenzetten waarom u geen FG heeft aangewezen. Op deze manier voorkomen zij dat u voor niets een FG aanstelt.



## ANDERE TIPS TER VOORBEREIDING OP DE AVG

1. Onderzoek welke maatregelen nu getroffen zijn. Uiteraard heeft Intermax deze informatie voor u wanneer wij uw IT-omgeving beheren. Wellicht is er voor uw eigen interne omgeving (denk aan laptops en andere apparatuur bij u op kantoor) nog een verbeterslag mogelijk.
2. Check welke persoonsgegevens u eigenlijk allemaal opslaat: welke 'kroonjuwelen' heeft u eigenlijk onder uw hoede? Welke gegevens zouden mensen gewist willen hebben? Hoe lang bewaart u gegevens? Kunt u nu al overbodige gegevens verwijderen?
3. Zorg dat u voldoende beschermingsmaatregelen treft. Dat kan op allerlei manieren, en hierbij kunnen wij u uiteraard helpen. Wij zorgen bijvoorbeeld al voor goede backup- en recoveryprocessen, maar er kan nog veel meer!
4. We kunnen u ook helpen om datastromen te monitoren; welke verbindingen met derden zijn er bijvoorbeeld? Denk aan VPN-tunnels, import-export procedures, extern opgeslagen back ups en bestanden etc. – deze kunnen en moeten scherp gevolgd worden!
5. Wanneer u geïnventariseerd heeft hoeveel gegevens u beheert kunt u ook vaststellen of het noodzakelijk is een Functionaris Gegevensbeheer aan te stellen.



 @Guardian360NL