CONSTANT &
VAN DEN HEUVEL
INCASSO & JURIDISCH ADVIES

Een leidraad voor de binnenkort in werking tredende:

Algemene Verordening Gegevensbescherming (AVG)

Inhoud **Pagina**

Uitleg omtrent benaming

De “General Data Protection Regulation” (GDPR) betreft nieuwe Europese wetgeving.
In verschillende landen heeft deze wetgeving een eigen benaming gekregen. Voor Nederland is dit: Algemene Verordening Gegevensbescherming (hierna “AVG”).

Het doel van de AVG

Het doel van de AVG is de bescherming van de persoonsgegevens van ieder natuurlijk persoon die een EU-burgerschap bezit.

Wanneer treedt de AVG in werking?

Per 1995 werd de eerste stap gezet met de “Data Protection Directive”, die in 1998 al eens werd vervangen door de “Data Protection Act”. In het jaar 2000 waren er ook al reguleringen nodig tussen de EU en de VS, welke de “Safe Harbor Privacy Principles” werden genoemd. Vanaf 2016 werd vervolgens bekend dat 25 mei 2018 de AVG in werking treedt. Omdat er ook een alternatief diende te komen voor de hierboven genoemde Safe Harbor Privacy Principles, vindt er dit jaar ook overleg plaats omtrent een “EU-VS Privacy Shield”. Alle bedrijven die gegevens verwerken van EU-burgers zullen hieraan moeten voldoen. ***25 mei 2018 is aldus de datum waarop de wet in werking treedt.***

Voor wie treedt de AVG in werking?

De AVG treedt in werking voor alle bedrijven, ongeacht omvang, die gegevens van EU-burgers verwerken.

Wat zijn (persoonlijke) gegevens van EU-burgers?

Uiteraard zijn dit in beginsel de NAW-gegevens, maar de scope is een stuk groter. Hieronder enkele voorbeelden, de lijst is officieel nog een stuk langer. Afhankelijk van de gegevens die uw bedrijf opslaat, zult u passende maatregelen moeten nemen.

Biografische gegevens:
Geboortedatum, BSN, strafblad, mailadressen, telefoonnummers, bank-informatie.
Uiterlijke gegevens:
Hoe je loopt, gezichtsherkenning, kleur ogen, haarkleur, lengte, gewicht et cetera.
Werk en Scholing:
Werkuren, salaris, certificaten en behaalde doelen, belastinginformatie et cetera.
Privéleven:
Foto’s, video’s, berichten, telefoongesprekken, IP-adressen, browsercookies, geloofsovertuiging et cetera.
Data mbt fysieke gesteldheid:
Ziektedagen, doktersbezoeken, medische geschiedenis, genetische data, allergieën et cetera.

De 7 data protectieprincipes

De data protectieprincipes die nagestreefd moeten worden, zijn:

1. Gerechtigd, Eerlijk en Transparant

Gerechtigd:

(a) Om te zorgen dat (persoons)data op een legale manier worden verwerkt, moet de persoon in kwestie (het "data subject") een **actieve** toestemming voor verwerking hebben gegeven;

(b) De verwerking van data moet nodig zijn om een afspraak/contract met het data subject uit te dienen;

(c) De verwerking van de data moet nodig zijn om mee te werken aan een actief legaal onderzoek waaraan het data subject moet voldoen;

(d) De verwerking van de data is nodig om de vitale gezondheid van het data subject te beschermen;

(e) De verwerking is nodig voor de uitvoering van taken van een autoriteit of overheidsinstantie;

(f) Het verwerken van de data is nodig vanwege de belangen aangegeven door de controleur van de data of een derde partij, behalve als zulke belangen worden overruled door de belangen van fundamentele rechten en vrijheid van het data subject, waarin bescherming van persoonlijke data en in het bijzonder de persoonlijke data van een kind worden geëist.

Eerlijk en Transparant:

(a) De organisatie moet zorgen dat het data subject weet wat en ook waarom zijn/haar data worden opgeslagen en waar deze voor gebruikt wordt;

(b) Het data subject heeft ook het recht te weten waar zijn/haar data worden opgeslagen;

(c) De data die worden opgeslagen moeten gelijk zijn aan de beschrijving.

2. Doel en limitatie

De persoonlijke data mogen enkel worden verwerkt voor het doel dat is aangegeven en waar het data subject zijn/haar akkoord voor heeft gegeven. Voor alle andere doelen mogen deze niet worden opgeslagen, zonder verkrijging van een aanvullend akkoord.

3. Minimale data

Er zal een minimale hoeveelheid data worden bewaard die voor het specifieke doel is aangegeven.

4. Correct

De opgeslagen data dienen correct te zijn en waar nodig up to date worden gebracht.

5. Opslaglimitatie

Data dienen niet langer opgeslagen te worden dan expliciet nodig is. Data welke niet meer noodzakelijk zijn dienen te worden verwijderd.

6. Integer en Vertrouwelijk

Data dienen te worden beschermd met alle mogelijke middelen tegen het ongeautoriseerd bewerken ervan, tegen per ongeluk verlies, tegen vernietiging en/of tegen beschadiging.

7. Verantwoordelijkheid

Er wordt een verantwoordelijke aangewezen voor de (opslag) van de data. Een controleur en de "verwerker"/processor zijn beiden verantwoordelijk voor de bescherming zoals de principes hiervoor aangeven. Uiteindelijk moet immers iemand verantwoording af (kunnen) leggen voor bovenstaande principes.

Autoriteiten

De Europese autoriteiten welke officieel verantwoordelijk zijn voor de GDPR/AVG-processen zijn:

1. de Europese Commissie
2. het Europees Parlement
3. de Raad van Ministers van de Europese Unie

Uiteindelijk heeft ieder (Europees) land zijn eigen verantwoordelijk instituut, of zal deze gaan krijgen. Voor Nederland is dit de Autoriteit Persoonsgegevens (AP)

De 7 rechten van een Data Subject

Onder de nieuwe wet heeft ieder persoon een aantal basisrechten:

1. ***Het recht om geïnformeerd te worden:***

Iedere EU-burger heeft het fundamentele recht om te weten door wie, waarom en hoe zijn/haar data zal worden en zijn verwerkt.

2. ***Het recht om toegang te krijgen tot zijn/haar eigen data:***

Iedere EU-burger heeft het recht om toegang te krijgen tot zijn/haar eigen data als het gaat om de volgende informatie:

(a) Het doel en de reden waarom de data worden verwerkt;

(b) Onder welke categorie de data vallen;

(c) De ontvangers of categorie van ontvangers naar wie de persoonlijke data zal worden gestuurd en/of daar toegang toe hebben;

(d) De mogelijkheid om van de controleur of verwerker van de data, rectificatie of verwijdering van de data te vragen;

(e) Het recht om hierover een klacht in te dienen bij de autoriteiten.

3. ***Het recht op rectificatie en correctie:***

Iedere EU-burger heeft het recht om zijn/haar data te laten rectificeren of corrigeren.

4. ***Het recht om te protesteren:***

Iedere EU-burger heeft het recht om te protesteren tegen verwerking van de gegevens, als het hierbij gaat om zijn/haar persoonlijke data.

5. ***Het recht om geen slachtoffer te worden van geautomatiseerde systemen:***
Iedere EU-burger heeft het recht om niet gewaardeerd en/of opgeslagen te worden op basis van keuzes gemaakt door geautomatiseerde systemen of profielen.

6. ***Het recht op data-overdracht:***
Iedere EU-burger heeft het recht om zijn/haar data van de ene controleur/verwerker naar de andere over te (laten) dragen.

7. ***Het recht op verwijdering (the right to be forgotten):***
De controleur of verwerker van de data is verplicht om zonder onnodige vertragingen de data van een data subject te verwijderen als:
(a) Dit niet in strijd is met de wet(ten) welke gelden in het land;
(b) Het data subject zijn of haar actieve toestemming intrekt;
(c) Het data subject hier om vraagt bij controleur en/of verwerker.

De Autoriteit, maar ook het datasubject, heeft enkele represailles tot haar of zijn beschikking

1. Reputatie schade.
   De organisatie zal hierdoor worden geschaad.
2. Recht op compensatie.
   Het data subject heeft het recht om via de autoriteiten of via juridische wegen compensatie te eisen.
3. Administratieve boete.
   De autoriteiten hebben het recht om een administratieve boete op te leggen tot:
   a. € 20.000.000,--
   b. 4% van de wereldwijde omzet.

Jurisdictie van AP (Autoriteit Persoonsgegevens)

Het is de verantwoordelijkheid van de AP om ervoor te zorgen dat de wetgeving omtrent dataprotectie wordt nageleefd. Ieder land binnen de EU heeft één of meerdere DPA (Data Protection Authorities) welke de plicht krijgen de implementatie van de GDPR/AVG te reguleren.

Taken van DPA:
(a) Controleren en monitoren of de wet wordt nageleefd;
(b) Bewustwording van personen en organisaties verhogen;
(c) Overheidsinstanties helpen met het implementeren van AVG-vereisten;
(d) Claims ingesteld door data subjects bekijken en classificeren;
(e) Opstellen en bewerkstelligen van duidelijk ”Impact Assessments”, oftewel een analyse van de mogelijke impact van beschikbare oplossingen.
(f) Ondersteuning van de code voor waarden en normen;
(g) Duidelijk documenteren van huidige en mogelijke sancties;
(h) Zorgen dat iedere bescherming van persoonlijke data wordt gewaarborgd.

Samenwerking binnen de DPA;
Omdat de AVG een Europese wetgeving is en ieder land zijn eigen “DPA” heeft, zorgt de DPA in het land waar het data subject zich begeeft voor een samenwerking binnen alle overige DPA. Daardoor creëert het systeem een “One-Stop-Shop” en ben je als data subject niet overgeleverd aan de grillen van verschillende overheidsorganen.

Buiten EU-gebied, toch data verwerken

Binnen de wetgeving GDPR/AVG bestaan er mogelijkheden dat data van EU-burgers toch buiten de grenzen van de EU geraken. Om ervoor te zorgen dat ook daar de bescherming van persoonsgegevens blijft gehandhaafd, heeft de EU een samenwerking met meerdere “Adequate” landen en/of aanvullende grensafspraken. Zo heeft de EU samen met de VS het “EU-US Privacy Shield” en bestaan er met lokale DPA buiten de EU-grenzen reeds afspraken met: Andorra, Argentinië, Canada, Zwitserland, Farao-eilanden, Israël, New-Zeeland en Uruguay.

Als het land waarin u data wilt verwerken niet op de “Adequate”-landenlijst staat (deze wordt geregeld bijgewerkt), betekent zulks dat er geen enkele manier is om GDPR af te dwingen binnen deze landen.

Tot zover de leidraad, doe er uw voordeel mee en bedenk dat het nieuwe wetgeving betreft die in de loop der tijd qua werking nader uitgekristalliseerd zal worden. Tot die tijd is het vaak een kwestie van gevoel zulks te vertalen naar uw eigen organisatie.