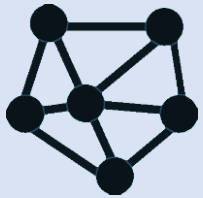
De Algemene Verordening Gegevensbescherming (AVG, in Europa onder de naam *General Data Protection Regulation*) is een ***centrale set regels*** die voor alle organisaties in de EU gelijk zijn en die geldt voor alle organisaties die ***actief*** in de EU zijn. Retailers, groot en klein, die on- en/of offline verkopen, verwerken in veel gevallen persoonlijke (klant- en/of personeels)data. ***De AVG is per 25 mei 2018 van toepassing.***

Data voorbeelden	***Wat precies?***		***Focus AVG voor de retail***
Klantgegevens 	NAW gegevens (ook *social media*), e.d.	**Extern**	Dataverwerking voor een retailer is bijvoorbeeld: - Invullen gegevens voor ***klantenkaart*** - NAW gegevens voor sturen van een ***mailing*** - ***Koophistorie*** gebruiken voor aanbiedingen
	Koophistorie, creditcard gegevens, betaaldata, klachtregistratie, e.d.		
	IP/MAC adressen, wachtwoorden, inloggegevens, e.d.		
Personeelsgegevens 	NAW gegevens	**Intern**	Een retailer is al een “data beheerder” wanneer het ***personeel*** in dienst heeft en is verantwoordelijk voor het juist behandelen van persoonlijke gegevens
	Salarissen, bonussen, e.d.		
	Functieomschrijving, e.d.		
	CV’s, cursussen, beoordelingen, promoties, ziekmeldingen, e.d.		

De Algemene Verordening Gegevensbescherming (AVG, in Europa onder de naam *General Data Protection Regulation*) is een ***centrale set regels*** die voor alle organisaties in de EU gelijk zijn en die geldt voor alle organisaties die ***actief*** in de EU zijn. Retailers, groot en klein, die on- en/of offline verkopen, verwerken in veel gevallen persoonlijke (klant- en/of personeels)data. ***De AVG is per 25 mei 2018 van toepassing.***

Inhoud	*Wat precies?*	*Impact retailsector*
Doelbinding	Als organisatie moet je kunnen uitleggen en beschrijven ***waarom*** je bepaalde persoonsgegevens verwerkt.	*Ieder persoon over wie je data op wilt slaan, moet hier expliciet toestemming voor geven. Bovendien geef je aan welke data je over die persoon opslaat en om welke reden.*
Consumentenrecht	De consument heeft t.a.t. recht op inzage en het ***intrekken*** van de toestemming op het verwerken van zijn persoonsgegevens.	*Wanneer een klant vraagt om zijn of haar gegevens te wijzigen of verwijderen, moet je hier vervolg aan geven.*
Data Portability	De consument heeft recht op ***inzage*** in de gegevens die zijn vastgelegd en heeft het recht zijn gegevens ***door te geven*** van organisatie A naar organisatie B.	*Het principe geldt hierbij: de persoonlijke gegevens zijn en blijven van de klant. De klant mag zijn of haar gegevens ook meenemen naar een andere organisatie.*
Informatieplicht	Consumenten moeten worden geïnformeerd dat persoonlijke gegevens worden verzameld en verwerkt.	*Bijvoorbeeld gegevens die nodig zijn om goederen te laten betalen en te verzenden, marketing informatie te sturen, het analyseren van koopgedrag.*

De Algemene Verordening Gegevensbescherming (AVG, in Europa onder de naam *General Data Protection Regulation*) is een ***centrale set regels*** die voor alle organisaties in de EU gelijk zijn en die geldt voor alle organisaties die ***actief*** in de EU zijn. Retailers, groot en klein, die on- en/of offline verkopen, verwerken in veel gevallen persoonlijke (klant- en/of personeels)data. ***De AVG is per 25 mei 2018 van toepassing.***

Inhoud	*Wat precies?*	*Impact retailsector*
Datalek	Binnen 72 uur na een ***datalek***, moet melding gemaakt worden bij de Autoriteit Persoonsgegevens (AP).	*Als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Bijvoorbeeld uitgelekte computerbestanden, cyberaanvallen (incl. DDos), e-mail verzonden naar verkeerde adressen, gestolen laptops, afgedankte niet-schoongemaakte computers, verloren usb-sticks, "hacks", etc.*
Data Protection Impact Assesment (DPIA)	Opstellen ***impact analyse*** op (bedrijfs)processen en risico's	*Vooraf aangeven welke processen als risicovol gezien worden en wat je doet om de kans te minimaliseren dat deze risico's zich inderdaad voordoen.*
Data Protection by Design & by Default	***Zichtbaar maken*** (d.m.v. de DPIA) dat het minimaliseren van de verwerking van persoonsgegevens centraal heeft gestaan by het design en inrichting.	*Vooraf aangeven dat minimaliseren van persoonsgegevens centraal heeft gestaan bij het ontwerp van je bedrijfsprocessen, website, etc.*
Beveiliging	Bedrijven moeten zorgen voor een gepaste ***beveiliging***.	*Je bent verplicht te controleren of de organisaties met wie je verwerkersovereenkomsten sluit, dat deze persoonsgegevens zorgvuldig beschermen tegen onbedoelde toegang. Als je zelf gegevens opslaat geldt dat direct voor jou als organisatie*

De Algemene Verordening Gegevensbescherming (AVG, in Europa onder de naam *General Data Protection Regulation*) is een ***centrale set regels*** die voor alle organisaties in de EU gelijk zijn en die geldt voor alle organisaties die ***actief*** in de EU zijn. Retailers, groot en klein, die on- en/of offline verkopen, verwerken in veel gevallen persoonlijke (klant- en/of personeels)data. ***De AVG is per 25 mei 2018 van toepassing.***

Inhoud	*Wat precies?*	*Impact retailsector*
Nauwkeurig	Persoonlijke data moeten ***nauwkeurig*** zijn en, indien nodig, geüpdatet worden. Persoonlijke data die niet nauwkeurig is (in relatie tot de doelen waarvoor ze verwerkt worden) moet worden ***gewist*** of ***gerectificeerd***.	*Je blijft altijd verantwoordelijk over de persoonsgegeven die je opslaat en verwerkt of laat verwerken.* *Denk aan wijzigingen in adresgegevens, betaalgegevens, maar ook personeelsgegevens (salarisverhoging, promotie).* *Geldt ook wanneer klanten hun persoonlijke gegevens willen laten verwijderen.*
Verantwoordelijke/*Data Protection Officer* (DPO) of Functionaris Gegevensbescherming (FG)	De bedrijfscontroller is er ***verantwoordelijk*** voor, dat het bedrijf handelt in overeenstemming met de AVG-principes. In sommige gevallen is het nodig een ***DPO/FG*** aan te stellen.	*De verwachting is dat alleen bedrijven die **op grote schaal grote hoeveelheden persoonsgegevens stelselmatig verwerken** een DPO/FG moeten aanstellen. Wel is het raadzaam dat er binnen een organisatie tenminste 1 persoon (in deeltijd) aanspreekpunt is voor de AVG naleving.*
Uitbesteden van verwerking persoonsgegevens	U kunt de verwerking van persoonsgegevens ook uitbesteden aan derde partijen.	*Wanneer u de verwerking van persoonsgegevens heeft uitbesteed aan een derde partij (bijvoorbeeld een salarisadministrateur, administratiekantoor, Payment Service Provider, etc.) dan bent u nog steeds verwerkingsverantwoordelijke.*

AVG en de Wet Bescherming Persoonsgegevens (Wbp)

(Oud) Onder de Wet Bescherming Persoonsgegevens (Wbp)

Verplicht om een overeenkomst af te sluiten met bewerkers

(Nieuw) onder AVG

De bewerker heeft nu ***verwerker***.
De AVG noemt een aantal verplichte onderdelen van deze overeenkomst:

- Het doel van de verwerking;
- Het soort persoonsgegevens dat wordt verwerkt;
- De categorieën van betrokkenen;
- Dat passende beveiligingsmaatregelen zullen worden genomen;
- Dat de verwerker meewerkt aan audits om te controleren of de verwerker zich aan alle verplichtingen houdt, en;
- Na afloop van de verwerking vernietiging of retourneren van de persoonsgegevens aan de verantwoordelijke;
- Verwerker mag niet meer een 3^{e} partij inschakelen zonder voorafgaande schriftelijke toestemming van de verantwoordelijke.

In een ***verwerkersovereenkomst*** staan bijvoorbeeld de volgende onderwerpen: toepasselijkheid en looptijd, verwerking (hoe en wat wordt verwerkt), beveiligingsmaatregelen, datalekprocedure, geheimhoudingsplicht, aansprakelijkheid.

Ga na welke verwerkers je inschakelt en welke afspraken er vastliggen. Zijn de verplichtingen uit de AVG voldoende gewaarborgd?

De Algemene Verordening Gegevensbescherming (AVG, in Europa onder de naam *General Data Protection Regulation*) is een ***centrale set regels*** die voor alle organisaties in de EU gelijk zijn en die geldt voor alle organisaties die ***actief*** in de EU zijn. Retailers, groot en klein, die on- en/of offline verkopen, verwerken in veel gevallen persoonlijke (klant- en/of personeels)data. ***De AVG is per 25 mei 2018 van toepassing.***

To Do list voor kleine retailer

- ✓ Kijk welke data waar en hoe verzameld, verwerkt en bewaard wordt
- ✓ Identificeer risico's, maak een risicoplan
- ✓ Treed in overleg met gegevensverwerkers die voor de eigen organisatie werken (bijvoorbeeld een Payment Service Provider, salarisverwerker, accountant, e-mail marketing provider, etc.) en stel een ***Verwerkersovereenkomst*** op of pas huidige aan
- ✓ Benoem 1 persoon als verantwoordelijke AVG naleving
- ✓ Zorg voor goede beveiliging van IT systemen
- ✓ Stel een nieuw privacy beleid in
- ✓ Stel een "Datalek Plan" op
- ✓ Update overeenkomsten met derde partijen/service providers indien nodig
- ✓ Communiceer privacy beleid naar werknemers en klanten
- ✓ Houdt berichten en informatie over de AVG goed in de gaten, bijvoorbeeld via Autoriteit Persoonsgegevens en brancheorganisatie

To Do list voor grote retailer

- ✓ Kijk welke data waar en hoe verzameld, verwerkt en bewaard wordt
- ✓ Identificeer risico's
- ✓ Treed in overleg met gegevensverwerkers die voor de eigen organisatie werken (bijvoorbeeld een Payment Service Provider, salarisadministrateur, accountant, e-mail marketing provider, etc.) en stel een ***Verwerkersovereenkomst*** op of pas huidige aan
- ✓ Benoem een Data Protection Officer (indien nodig) of een eindverantwoordelijke
- ✓ Organiseer privacy trainingen voor werknemers
- ✓ Stel Data Protection Impact Assessment (DPIA) of gegevensbeschermingseffectbeoordeling op
- ✓ Zorg voor goede beveiliging van IT systemen
- ✓ Stel een "Datalek Plan" op
- ✓ Update overeenkomsten met derde partijen/service providers indien nodig
- ✓ Zorg voor goede beveiliging van IT systemen
- ✓ Stel nieuw privacy beleid in
- ✓ Communiceer privacy beleid naar werknemers en klanten
- ✓ Houdt berichten en informatie over de AVG goed in de gaten, bijvoorbeeld via Autoriteit Persoonsgegevens en brancheorganisatie

Datalekken

(Oud) Onder Wbp	*(Nieuw) onder AVG*
Meldplicht datalekken Onder de Wbp moet er al een melding worden gedaan als niet kan worden uitgesloten dat er een onrechtmatige verwerking van persoonsgegevens kan plaatsvinden.	De verwerker is onder de AVG verplicht een datalek te melden aan de verantwoordelijke (bijvoorbeeld de opdrachtgever). Er hoeft pas een melding bij de toezichthouder gedaan te worden als er **daadwerkelijk** een lek heeft plaatsgevonden.

Voor organisaties betekent dit een aantal extra verplichtingen, zoals:

- Het digitaal overdragen van persoonsgegevens aan een andere partij, bijvoorbeeld een leverancier of concurrent. De digitale overdracht moet beveiligd zijn;
- Het hebben van een gegevensbeschermingsbeleid;
- Verantwoordelijkheid voor de keten van verwerkers;
- Het aanleggen van een register van verwerkingsactiviteiten;
- Documentatie van alle datalekken;
- Uitvoering van een ‘Gegevensbeschermings-effectbeoordeling’, beter bekend als de *Privacy Impact Assessment* (PIA).

Boetes bij overtredingen kunnen oplopen tot €20 mln of 4% van de jaaromzet

Detailhandel Nederland

Detailhandel Nederland behartigt de collectieve sociale en economische belangen van de winkeliers. Het doel is om het perfecte klimaat te creëren waarbinnen winkeliers optimaal kunnen ondernemen. Door de samenwerking in Detailhandel Nederland kunnen het midden- en kleinbedrijf (MKB) en grootwinkelbedrijf (GWB) gezamenlijk met een standpunt naar buiten treden. Dit versterkt de belangenbehartiging van de detailhandel bij de Nederlandse en Europese overheid.
Detailhandel Nederland is een samenwerkingsverband van NWR, CBL en RND. De volgende brancheverenigingen zijn verbonden: