# General Data Protection Regulation.

## Bent u al voorbereid op de nieuwe Europese Data Protectie wetgeving?

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie. De Wet Bescherming Persoonsgegevens (WBP) geldt dan niet meer.

De AVG is ook wel bekend onder de Engelse naam: General Data Protection Regulation (GDPR). De GDPR is ontwikkeld omdat de Europese Unie een eenduidige en veilige Europese digitale omgeving voor burgers wil garanderen. De nieuwe privacywet heeft invloed op elke onderneming die persoonlijke data gebruikt van Europese burgers.

## Algemene Verordening Gegevensbescherming (AVG)

De nieuwe privacywetgeving gaat een stap verder dan de vorige Wet Bescherming Persoonsgegevens. De Algemene Verordening Gegevensbescherming (AVG) is de Nederlandse vertaling van de GDPR en verscherpt regels uit de huidige Wet Bescherming Persoonsgegevens, maar voegt ook een aantal nieuwe verplichtingen toe. Wat dit precies voor u in de praktijk betekent, hebben wij voor u samengevat in deze white paper.

De belangrijkste consequentie van GDPR is dat bedrijven veel bewuster met data om moeten gaan. Dat betekent dat alleen onder strikte voorwaarden persoonlijke informatie over bijvoorbeeld: leeftijd, sekse, woonplaats en religie mogen worden verzameld en bewaard. Het begrip ‘persoonsgegevens’ wordt in de GDPR ruimer omschreven en geldt ook wanneer een persoon met behulp van een (online) identificator (bijvoorbeeld een IP-adres of kenteken) geïdentificeerd kan worden, of geïsoleerd kan worden uit een groep.

## Duidelijk vragen om toestemming

Toestemming moet onder de GDPR een ‘ondubbelzinnige’ wilsuiting zijn. Dit houdt in dat toestemming uit een actieve handeling moet bestaan. Dus geen vooraf aangevinkte hokjes meer maar een duidelijke vraag (in eenvoudig Nederlands) om toestemming. Als er toestemming voor meerdere doeleinden wordt gevraagd, dan moet daarvoor apart goedkeuring worden gevraagd.
Bedrijven moeten uiteindelijk kunnen bewijzen dat de betrokkene toestemming heeft gegeven. De betrokkene heeft te allen tijde het recht de toestemming in te trekken en moet daar ook op worden gewezen.

De GDPR introduceert kernbeginselen waaraan alle verwerkingen van persoonsgegevens moeten voldoen:

- Persoonsgegevens moeten op behoorlijke, rechtmatige en transparante manier worden verwerkt.
- Persoonsgegevens mogen alleen voor een bepaald, uitdrukkelijk omschreven doel worden verwerkt.
- Alleen persoonsgegevens die noodzakelijk zijn voor het doel mogen worden verwerkt.
- Gegevens moeten correct en actueel zijn.
- Als identificatie niet meer noodzakelijk is voor het doel, dan moeten de persoonsgegevens worden verwijderd of geanonimiseerd.
- De persoonsgegevens moeten worden beveiligd door middel van technische en organisatorische maatregelen.

Het is duidelijk dat met de aangescherpte wetgeving consumenten meer invloed hebben op de informatie die bedrijven hebben opgeslagen. De GDPR geldt echter ook voor alle data die een bedrijf opslaat van haar klanten (B2B).

## Wat betekent de GDPR voor u in de praktijk?

De regelgeving stelt dat er zo min mogelijk gegevens bewaard mogen worden en bedrijven moeten zelf beoordelen of het datagebruik gerechtvaardigd is of niet. De wet heeft betrekking op alle data geregistreerd over natuurlijke personen binnen Europa, ongeacht waar de data wordt opgeslagen. Met andere woorden: ook data opgeslagen in datacenters in de Verenigde Staten, Rusland en China moeten aan de GDPR voldoen. Bedrijven moeten bovendien aan kunnen tonen dat ze zich aan de regels houden. Iedereen die zich niet aan deze voorwaarden houdt is strafbaar. Voor alle (persoons)data die u opslaat moet u in ieder geval de volgende punten kunnen verdedigen:

- **Waarom** worden deze persoonsgegevens verwerkt (en dus gevraagd).
- **Welke** persoonsgegevens worden verwerkt.

- **Met wie** wordt deze informatie gedeeld.
- **Hoelang** worden de gegevens opgeslagen.
- Ieder persoon waarvan gegevens opgeslagen zijn moet deze (exacte) gegevens **kunnen opvragen, aanpassen en verwijderen.**
- **Hoe wordt de privacy gewaarborgd** als dataopslag buiten de EU plaatsvindt.

In de huidige privacywetgeving is reeds vastgelegd dat testdata niet herleidbaar mag zijn naar echte persoonsgegevens in de productieomgeving. De GDPR scherpt deze regels verder aan. Worden bijvoorbeeld opgeslagen persoonsgegevens gebruikt om een service te verlenen, dan kan deze data niet zomaar gebruikt worden om de applicatie waarmee de data vergaard wordt te testen.
Om zeker te stellen dat de opgeslagen persoonsgegevens veilig zijn, gaat GDPR uit van 'Privacy by design'. Dit houdt in dat de applicatie en het verkeer tussen de applicatie en de database ontworpen moeten zijn om veilig data te vergaren en op te slaan door diverse encryptielagen en andere vormen van beveiliging toe te passen. Daarnaast moeten de standaardinstellingen van het systeem zo privacy-vriendelijk mogelijk zijn en mogen er niet meer persoonsgegevens worden verwerkt dan noodzakelijk (Privacy by Default).

## Privacy borgen in uw organisatie

Om de veiligheid van data te waarborgen moet bij ieder bedrijf de rol van Data Protection Officer duidelijk belegd te zijn. Dit hoeft niet per se een eigen medewerker te zijn; de rol mag ook worden vervuld door een externe consultant of bijvoorbeeld een software security expert. De Data Protection Officer is verantwoordelijk voor alle processen rond data, dataopslag en data- overdracht. Daarnaast dient deze persoon zicht te hebben op het (on)eigenlijk gebruik van data. Denk hierbij aan niet geanonimiseerde data op test- en ontwikkelomgevingen.
Op dit moment bestaat in Nederland de meldplicht van databreaches. Deze plicht blijft binnen de GDPR bestaan. Elke vorm van datalek zal dus ook in de toekomst gemeld moet worden. Een datalek houdt niet alleen in dat er productiedata "op straat" ligt, maar kan ook testdata betreffen, als deze gebaseerd is op productiedata en daarmee te herleiden is naar echte personen. De Data Protection Officer is verantwoordelijk voor het opstellen van regels hoe een data lek gemeld wordt, door wie deze gemeld wordt et cetera.

## Hoe kan Polteq u helpen?

Met onze specialistische kennis op het gebied van gestructureerd testen, datawarehouse testen en security testen kan Polteq door middel van een audit of security test datarisico's in kaart brengen. De testprofessionals van Polteq zijn allemaal getraind om zich te verplaatsen in de eindgebruiker. Dit stelt ze in staat om heel goed vast te stellen of de opgevraagde en opgeslagen persoonsgegevens voor hen, als eindgebruiker, logisch te verklaren zijn. Daarnaast kunnen de testprofessionals helpen bij het gedegen testen van de audit trails op de opgeslagen persoonsgegevens.

Onze specialisten hebben veel ervaring in het testen van de autorisatie- en authenticatiemodellen en applicaties die gebruikt worden om de data in de applicatie af te schermen van oneigenlijk gebruik. Daarnaast kunnen de security testers van Polteq ingezet worden als Data Protection Officer binnen uw organisatie. Zij kunnen helpen met het opstellen van een Databreach-plan, het uitvoeren van Privacy Impact Assessments en Data Protection Impact Assessments.

*Kortom; de AVG komt eraan en snel ook! Meer dan voorheen worden bedrijven en organisaties geacht te kunnen aantonen dat zij zich aan de wet houden. Dit vergt een goede voorbereiding. Als organisatie kunt u nu al stappen ondernemen om straks klaar te zijn voor de AVG en wij helpen u daar graag bij! Wilt u meer weten, neem dan contact met ons op.*