De AVG is al even van kracht, maar vanaf 25 mei 2018 zal de Autoriteit Persoonsgegevens ook op deze verordening gaan controleren. De AVG is een Europese regeling en vervangt de huidige Wet bescherming persoonsgegevens.

**Voor alle ondernemers**
De AVG geldt voor alle ondernemers en heeft betrekking op het verwerken van alle persoonsgegevens, dus naast klanten bijvoorbeeld ook uw personeelsleden.

De AVG regelt -kort samengevat- dat u als ondernemer:

1. Een grondslag moet hebben én kunnen aantonen, waarom u gerechtigd bent persoonsgegevens te verwerken. Die grondslag zal -in uw praktijk- doorgaans zijn:
a. Uitdrukkelijk gegeven toestemming die vrijwillig en ondubbelzinnig is gegeven, voor het specifieke doel waarvoor u de gegevens wilt verwerken of met wie u deze deelt. U dient deze persoon onder meer duidelijk te informeren over welke gegevens u verzamelt en gebruikt, waar u ze voor gaat gebruiken en dat men het recht heeft deze toestemming weer in te trekken.
In de praktijk: vermeld deze informatie op uw website (Privacyverklaring, zie ook 4 d), laat mensen actief aanvinken dat men toestemming verleent voor het verwerken van hun gegevens en vermeld waarvoor u deze gegevens gaat gebruiken.
b. De gegevens zijn noodzakelijk voor de uitvoering van een overeenkomst.
Besef dat deze grondslag alleen geldt voor persoonsgegevens die echt noodzakelijk zijn voor de uitvoering van de overeenkomst. Gaat u de gegevens ook voor een mailing gebruiken, dan moet daar (zie a) uitdrukkelijke toestemming voor gegeven worden.
In de praktijk: houd goed in de gaten dat alleen noodzakelijke gegevens worden gevraagd en vastgelegd. Om elke discussie te voorkomen is het raadzaam om ook (aanvullende) toestemming te vragen (zie a).
Het is vereist om -op verzoek- aan te kunnen tonen dat u aan de voorstaande grondslagen heeft voldaan. Bij het aantonen van de gegeven toestemming (zie a) moet ook de informatie vastgelegd worden die de persoon is verstrekt.

2. Grote organisaties (en dus ook de overheid), organisaties die medische of andere gevoelige informatie verwerken, grote hoeveelheden persoonsgegevens verwerken, personen volgen of op een andere manier een groot privacyrisico lopen, moeten aan extra eisen voldoen. Zoals het aanstellen van een Functionaris gegevensbescherming of periodiek een Data protection impact assessment doen. Voor de juweliersbranche zullen deze aspecten van de verordening geen rol spelen.

3. Als ondernemer zult u bepaalde zaken moeten regelen:
a. Hoewel de AVG nog een uitzondering lijkt te maken voor kleine ondernemingen, moet feitelijk iedereen die bepaalde gegevens structureel verwerkt een Register van verwerkingsactiviteiten bijhouden. Dit is niet meer dan een bestand waarin staat opgenomen wie u bent, waarvoor u de gegevens verwerkt, een beschrijving van categorieën van personen én (soort) persoonsgegevens die worden verwerkt, met wie u deze gegevens deelt, hoe lang u ze bewaart, op grond waarvan u toestemming heeft deze te bewaren én de wijze waarop u de gegevens heeft beveiligd.
In de praktijk: stel een overzicht op, waarin deze informatie -duidelijk- staat omschreven.
b. De beveiliging van gegevens verdient extra aandacht. De AVG schrijft voor dat het beveiligingsniveau moet zijn afgestemd op de risico’s die de gegevensverwerking met zich meebrengt. Des te gevoeliger de gegevens zijn die u verwerkt, des te zwaarder de eisen zijn.
In de praktijk: beperkt het aantal personen die toegang hebben tot de gegevens en verander wachtwoorden regelmatig. En als het niet noodzakelijk is om de gegevens online te bewaren, doet dat dan niet. Test zelf periodiek of de gegevens naar de stand van de techniek nog voldoende beveiligd zijn.
c. Kleine organisaties die niet op grote schaal persoonsgegevens verwerken, zijn niet verplicht om een gegevensbeschermingsbeleid of privacybeleid op te stellen. Dit onderdeel laat ik dan ook rusten, maar zal onder 4d gedeeltelijk terugkomen.

4. Tenslotte hebben de personen waarvan u de gegevens verwerkt grote zeggenschap over hun persoonsgegevens. Denk aan:
a. Het recht op inzage. Dit wil zeggen dat u op verzoek van een persoon moet aangeven waarom u bepaalde gegevens verwerkt, welke gegevens u verwerkt, met wie u deze gegevens deelt, hoe lang u deze gegevens bewaart én dat men tevens het recht heeft op:
b. Het recht van rectificatie. Mochten gegevens niet kloppen, dan moet u deze op verzoek van een persoon aanpassen én dit direct doorgeven aan de organisaties waarmee u deze gegevens deelt;
c. Het recht om vergeten te worden. Persoonsgegevens moeten gewist worden, wanneer iemand daarom vraagt. Aan dit verzoek hoeft niet altijd gehoor gegeven te worden, maar wél wanneer het gaat om gegevens die niet meer nodig zijn om te bewaren of die te maken hebben met het intrekken van een gegeven toestemming (denk aan een mailinglist);
d. Tenslotte rust op u een informatieplicht. U bent verplicht om nieuwe en bestaande klanten duidelijk te informeren over wat u met hun persoonsgegevens doet. De makkelijkste manier is via een privacyverklaring op uw website. In deze verklaring moet duidelijk worden uitgewerkt wat u met de persoonsgegevens doet. Ontvangt u de persoonsgegevens offline, bijvoorbeeld op een reparatiezakje, dan zou u daarop uw privacyverklaring moet opnemen.
In de praktijk: de meeste van deze verplichtingen zijn (logische) rechten van een persoon. Het opstellen en gebruiken van een privacyverklaring is raadzaam.

**Waar moet u beginnen?**
De AVG vraagt van u om bewust met (privacygevoelige) persoonsgegevens om te gaan.
- Kijk daarom eerst wélke gegevens u heeft verzameld, wát u ermee doet en of dat allemaal noodzakelijk is. Het verstrekken van de persoonsgegevens van een klant aan een reparateur is bijvoorbeeld niet noodzakelijk;
- Stel een Register van verwerkingsactiviteiten op (zie 3a);
- Ga na of u de vereiste (uitdrukkelijke) toestemmingen heeft om de persoonsgegevens op te slaan;
- Ga na hoe u de beveiliging van deze gegevens heeft geregeld;
- Houd in de gaten dat de personen waarvan u de gegevens verwerkt grote zeggenschap hebben over hun gegevens;
- Informeer uw klanten duidelijk over wat u met hun persoonsgegevens doet en stel een privacyverklaring op.

Meer informatie is ook te vinden op [www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl).

mr. W.J.M. (Bart) Sprangers, Kuijpers Advocaten