Stappenplan

1. Stel vast wie in uw bedrijf de personen zijn die de meeste kennis hebben van de (persoons)gegevens die worden verwerkt (dat wil zeggen; verzamelen en opslaan).
2. Kijk samen met deze personen wélke gegevens u verzamelt, wát u ermee doet en of dat allemaal noodzakelijk is. Het verstrekken van de persoonsgegevens van een klant aan een reparateur is bijvoorbeeld niet altijd noodzakelijk.
3. Breng alle gegevens die u verwerkt in kaart (in lijn met de [vereisten](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/verantwoordingsplicht#wat-moet-er-in-het-register-van-verwerkingsactiviteiten-staan-6137) die aan een Register van Verwerkingsactiviteiten worden gesteld) én stel vast of deze gegevens door u mogen worden verwerkt. Hierbij is de 'grondslag' waarop u gegevens verwerkt bepalend. De grondslagen waarop u gegevens mag verwerken zijn bijv. 'gerechtvaardigd belang', 'wettelijke plicht', 'uit overeenkomst' of 'gegeven toestemming'. In de sieraden- en horlogebranche worden voornamelijk NAW-gegevens en e-mailadressen van klanten verwerkt met als grondslag ‘uit overeenkomst’. Dit geldt ook voor de persoonsgegevens van uw medewerkers; die verzamelt u op grond van de arbeidsovereenkomst. De invoer van gegevens in het (digitale) opkoopregister heeft als grondslag ‘wettelijke plicht’. Het verwerken van gegevens zoals teksten voor gravures en ringmaat vloeit voort uit de overeenkomst of heeft als grondslag gerechtvaardigd belang bij de uitvoering van de overeenkomst. Ook cameratoezicht heeft als grondslag gerechtvaardigd belang.
4. Stel een Register van Verwerkingsactiviteiten op n.a.v. stap 3. Hiervoor kunt u het voorbeeld van een Register gebruiken dat u hier kunt downloaden. Let op: het voorbeeld is opgesteld op basis van de meest voorkomende gegevensverwerkingsactiviteiten in een juweliers-, goudsmids- of uurwerkreparatiebedrijf; het is uw eigen verantwoordelijkheid om na te gaan of het Register hiermee voor uw bedrijf compleet is. In het voorbeeld-register staat ook een verwijzing naar een bijlage met een overzicht van de partijen waarmee de bedrijven in de branche vaak gegevens delen (ook hier geldt dat het uw eigen verantwoordelijkheid is om na te gaan of dit overzicht voor uw bedrijf compleet is). Het opstellen van een dergelijk Register is niet voor alle bedrijven verplicht. Het valt echter wel voor iedereen aan te raden: als u gecontroleerd wordt kunt u hiermee laten zien hoe u met de privacyregels omgaat (verantwoordingsplicht). Dit geldt ook als een klant inzage vraagt in de gegevens die u van  hem of haar verzamelt en wat u daarmee doet.
5. Ga waar nodig na of u de vereiste (uitdrukkelijke) toestemmingen heeft om de persoonsgegevens op te slaan en te verwerken. Van iemand die met u een koop- of reparatieovereenkomst heeft gesloten mag u de noodzakelijke contactgegevens verzamelen op grond van de overeenkomst die deze persoon met u heeft gesloten. Van iemand die alleen uw website heeft bezocht mag u gegevens alleen verzamelen als u dat duidelijk aangeeft. U mag bijvoorbeeld pas iemand een mailing sturen, wanneer de betreffende persoon daar zelf uitdrukkelijke toestemming voor heeft gegeven. U mag cookies gebruiken die noodzakelijk zijn voor het functioneren van uw website (zoals wat er in het winkelwagentje zit en wanneer iemand is ingelogd). Voor het gebruik van andere cookies dan deze functionele cookies moet u toestemming vragen aan de bezoeker van uw website (zoals cookies die klikgedrag bijhouden, die meten hoe lang iemand op een pagina is, waarmee je bezoekers laat reageren via social media of die meten of iemand een advertentie heeft gezien). U moet ook de mogelijkheid bieden om uw website te bezoeken zonder dat de bezoeker toestemming geeft voor niet-functionele cookies. Vraag om advies bij uw websitebeheerder.
6. Ga na of u de beveiliging van de gegevens die u verzamelt goed heeft geregeld.
7. Informeer uw klanten duidelijk over wat u met hun persoonsgegevens doet door middel van een Privacyverklaring waarin u uw privacy-beleid omschrijft (publiceer de Privacyverklaring op uw website en in uw winkel). Hiervoor kunt u het voorbeeld van een Privacyverklaring gebruiken dat u hier kunt downloaden. Let op: het voorbeeld is opgesteld op basis van de meest voorkomende gegevensverwerkingsactiviteiten in een juweliers-, goudsmids of uurwerkreparatiebedrijf; het is uw eigen verantwoordelijkheid om na te gaan of de Privacyverklaring hiermee voor uw bedrijf compleet is.
8. Waarschijnlijk hebben uw medewerkers toegang tot uw klantgegevens. Daarom moeten ook zij op de hoogte zijn van uw privacy-beleid en ervoor tekenen dat zij zich hieraan zullen houden (door een artikel in hun arbeidsovereenkomst of als aparte verklaring (geheimhoudingsovereenkomst). Een tekst die u daarvoor kunt gebruiken, kunt u hier downloaden.
9. U mag berichten aan uw bestaande klanten sturen mits u hen de mogelijkheid biedt om aan te geven dat ze daar geen prijs meer op stellen (een zgn. “opt-out”-mogelijkheid). Voor de zekerheid kunt u een zgn. her-activatiemailing sturen aan de overige personen op uw mailinglist en hen vragen of ze er nog steeds toestemming geven dat u ze berichten en e-mailingen stuurt. Veel software voor e-mailings maakt standaard melding van de “opt-in” en “opt-out” mogelijkheid.
10. Check hier of u verplicht bent om een 'Data protection impact assessment' te doen of een 'Functionaris voor de gegevensbescherming' aan te stellen (let op: voor de gemiddelde MKB’er is dat niet nodig).
11. Laat u gegevens door een derde partij 'verwerken' (zonder dat die derde partij die gegevens voor een eigen doel gebruikt)? Stel dan een Verwerkersovereenkomst op met die partij. Hiervoor kunt u het voorbeeld van een Verwerkersovereenkomst gebruiken dat u hier kunt downloaden). Indien de derde partij de gegevens voor een eigen doel gebruikt (bijvoorbeeld een horlogemerk dat de gegevens gebruikt voor de aanspraak van consumenten op fabrieksgarantie) dan is de derde partij zelf verantwoordelijk voor deze gegevens en hoeft u geen Verwerkersovereenkomst op te stellen.
12. Doorloop alle “kanalen” waardoor persoonsgegevens binnenkomen (of kunnen lekken) en check of die afdoende “afgedekt” zijn met (technische) beveiligingen, overeenkomsten, privacyverklaringen en (indien noodzakelijke) uitdrukkelijk toestemming.
13. Blijf continu alert op uw verantwoordelijkheid de persoonsgegevens veilig en doelmatig te gebruiken en meld datalekken. Houd in de gaten dat de personen waarvan u de gegevens verwerkt grote zeggenschap hebben over hun gegevens.