FEDERATIE NEDERLANDSE RUBBER- EN KUNSTSTOFINDUSTRIE

Postbus 420
2260 AK Leidschendam

Tel: (070) 444 06 60
Fax: (070) 444 06 61

Synthesium gebouw C
Loire 150, 2491 AK Den Haag

E-mail: info@nrk.nl
Website: www.nrk.nl

Algemene Verordening Gegevensbescherming

Vanaf 25 mei 2018 geldt de nieuwe Algemene Verordening Gegevensbescherming (AVG). Deze privacywetgeving is van toepassing op het verzamelen, verwerken, bewaren en doorgeven van persoonsgegevens.

Hierna worden de belangrijkste zaken op een rij gezet.
Met dank aan Stb Automatisering en Advies voor toestemming voor het gebruik van het door hen opgestelde praktisch naslagwerk.

- Veel informatie is te vinden op de website van de Autoriteit Persoonsgegevens. https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving

- Op de website van RVO staat een speciale regelhulp AVG voor bedrijven. https://rvo.regelhulpenvoorbedrijven.nl/avg/#/welkom

- Op de website van veiliginternetten.nl staat een privacyverklaring generator. https://veiliginternetten.nl/privacyverklaring/

1. Wie krijgt met de AVG te maken?
De AVG is van toepassing op iedere organisatie die persoonsgegevens beheert, opslaat of (laat) verwerken.

2. Wanneer moet een privacy-officer worden aangesteld?
Een privacy-officer is verplicht voor overheidsorganisaties en organisaties die op grote schaal gevoelige persoonsgegevens verwerken of personen structureel observeren (cameratoezicht). Bij de meeste MKB-bedrijven en verenigingen is geen privacy-officer nodig.

3. Wanneer moet een privacy impact assessment (pia) worden uitgevoerd?
Als gegevensverwerking een hoog privacy-risico oplevert moet een pia worden uitgevoerd. Voor de meeste verenigingen en MKB-bedrijven is een pia niet nodig.
Zie bijlage 1 voor verdere uitleg.

4. Wanneer mogen persoonsgegevens worden vastgelegd?
Persoonsgegevens mogen alleen worden verwerkt op basis van een wettelijke grondslag. Dat kan zijn: toestemming, een wettelijke verplichting, een overeenkomst, het algemeen belang, een vitaal belang of een gerechtvaardigd belang.

Bijzondere persoonsgegevens (zoals gezondheid, etnische afkomst, geaardheid, levensbeschouwing, vakbondslidmaatschap, politieke opvatting, strafbare feiten of veroordeling of daarmee verband houdende veiligheidsmaatregelen), mogen alleen worden verwerkt indien aan een van de volgende voorwaarden voldaan is.
Dat kan zijn: toestemming: noodzakelijke verwerking vanwege verplichtingen uit het arbeidsrecht of sociale zekerheidsrecht; noodzakelijk vanwege preventieve geneeskundige doeleinden, beoordeling arbeidsgeschiktheid werknemer; algemeen belang gezondheidszorg; noodzakelijk voor rechtsvordering; door de persoon zelf openbaar gemaakte gegevens; bescherming vitale belangen; verwerking door kerk of vakbond; zwaarwegend algemeen belang; noodzakelijk voor archivering in kader algemeen belang).

N.B. Bij toestemming moet dat een actieve handeling van de persoon zelf zijn. Het vermelden in de algemene voorwaarden is rechtsgeldig.
Zie bijlage 2 en 3 voor verdere uitleg.

5. Wanneer is er een verwerkingsregister verplicht?
Organisaties van meer dan 250 werknemers zijn verplicht een verwerkingsregister aan te leggen. Dat geldt ook voor organisaties met minder dan 250 personen indien deze bijzondere en/of privacygevoelige en/of de verwerking niet incidenteel is.

Bij veel verenigingen en MKB-bedrijven zal de verwerking niet incidenteel zijn. Dan is een verwerkingsregister nodig. Zie bijlage 4 voor verdere uitleg.

Bedrijven wordt aangeraden om een overzicht op te stellen van de verschillende gegevensbestanden die zijn hebben, wie dat betreffen, wat geregistreerd wordt, waarom, op welke grondslag, hoe lang de gegevens worden bewaard en of de gegevens verwijderd c.q. aangepast mogen worden. In Bijlage11 vindt u een opzet voor zo'n overzicht.

6. Mag een externe partij persoonsgegevens voor mij verwerken?
De organisatie mag de persoonsgegevens zelf verwerken maar, onder haar verantwoordelijkheid, ook door een derde partij laten verwerken. Wel moet met de derde partij een verwerkersovereenkomst worden afgesloten. Zie bijlage 12 voor meer informatie.

7. Wat als meerdere organisaties dezelfde database gebruiken?
Als twee of meer organisaties persoonsgegevens in een gezamenlijke database verwerken, moete tussen deze organisaties een onderlinge regeling worden opgesteld, waarin de verantwoordelijkheden en verplichtingen uit de AVG zijn beschreven.

8. Moeten organisaties een privacyverklaring opstellen?
Organisaties moeten een privacyverklaring opstellen, waarin in een eenvoudige taal wordt uitgelegd wat de organisatie met de persoonsgegevens doet. De doeleinden van verwerking moeten erin staan, de grondslag van verwerking, wie de gegevens ontvangt en hoe lang de gegevens worden bewaard. Verder moet de verklaring duidelijkheid geven over de rechten van de personen etc. Zie bijlage 5 voor verdere informatie.

9. Wat te doen als persoonsgegevens zijn verloren , gehackt of gelekt?
Alle datalekken moet intern worden vastgelegd. Ernstige datalekken moeten bij de Autoriteit Persoonsgegevens worden gemeld. In sommige gevallen moeten ook de personen van wie de persoonsgegevens zijn gelekt, op de hoogte worden gebracht.

10. Wat is privacy by design en privacy by default?
Privacy by design houdt in dat de organisatie al tijdens de ontwikkeling van producten en diensten aandacht besteedt aan privacyverhogende maatregelen en rekening houdt met dataminimalisatie: alleen de gegevens die strikt noodzakelijk zijn worden verwerkt.
Privacy by default houdt in dat standaardinstellingen (bijvoorbeeld op de website) altijd zo privacyvriendelijk mogelijk moeten zijn ingesteld.

11. Wat voor procedures voor gegevensbeveiliging en procedures voor inzage etc.
Zorg binnen de organisatie ervoor dat duidelijk is wie welke persoonsgegevens mag inzien en verwerken. Zorg ervoor dat gegevens veilig worden opgeslagen en door medewerkers op een juiste wijze worden gebruikt. Zie bijlage 6 voor verdere informatie.

Zorg voor procedures zodat personen hun gegevens: kunnen inzien, om rectificering kunnen vragen, laten wissen, overdracht van gegevens te beperken of hun gegevens over te dragen. Voorbeelden staan in bijlagen 7, 8 en 9. In bijlage 10 staan de belangrijkste definities.

12. Wat zijn de consequenties van het niet voldoen aan de AGV?
De Autoriteit Persoonsgegevens (AP) krijgt aanzienlijk meer sanctioneringsmogelijkheden om naleving van de verordening te handhaven. Dit kan in de vorm van het opleggen van hoge boetes die voldoende afschrikkend zijn. De AP kan een boete opleggen van maximaal 20 miljoen euro. Of een boete van 4% van de wereldwijde jaaromzet, mocht dat bedrag hoger uitkomen. Ook het verbieden van verwerkingen van persoonsgegevens behoort tot de mogelijkheden.

Bijlage 1: Protection Impact Assessment (PIA)

Een organisatie is verplicht tot het uitvoeren van een data protection impact assessment (PIA) als gegevensverwerking waarschijnlijk een hoog privacy-risico oplevert voor de personen van wie gegevens verwerkt worden. Van zo een risicovolle verwerking is volgens de AVG in ieder geval sprake als:

- systematisch en uitvoerig persoonlijke kenmerken evalueert, waaronder profiling;
- op grote schaal bijzondere persoonsgegevens verwerkt;
  (bij de grootschaligheidsbeoordeling wordt gekeken naar het aantal mensen van wie gegevens worden verwerkt, de hoeveelheid gegevens die worden verwerkt, de duur van de gegevensverwerking en de geografische reikwijdte van de verwerking)
- op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

Valt de verwerking niet onder de drie bovengenoemde criteria dan, zal de organisatie zelf een beoordeling moeten maken of een PIA noodzakelijk is. Kijk hierbij naar de aard, omvang, context en het doel van de (voorgenomen) verwerking.

Een werkgroep van Europese Privacy-toezichthouders heeft een tiental criteria opgesteld. Voldoet een organisatie aan drie of meer van deze criteria dan is een PIA noodzakelijk.

1. Beoordelen van mensen op basis van persoonskenmerken
2. Geautomatiseerde beslissingen
3. Stelselmatige en grootschalige monitoring
4. Gevoelige gegevens
5. Grootschalige gegevensverwerkingen
6. Gekoppelde databases
7. Gegevens over kwetsbare personen
8. Gebruik van nieuwe technologieën
9. Doorgifte van persoonsgegevens buiten de EU
10. Blokkering van een recht, dienst of contract

Bijlage 2: Wanneer mogen gewone persoonsgegevens worden vastgelegd?

De verwerking van persoonsgegevens (bijzondere persoonsgegevens uitgezonderd) is rechtmatig als ten minste aan een van de onderstaande voorwaarden is voldaan:

1. Toestemming:
   De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden.
2. Noodzakelijk uitvoering overeenkomst
   De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen.
3. Wettelijke verplichting/publieke taak
   De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.
4. Bescherming vitale belangen
   De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen.
5. Algemeen belang/gezaguitoefening
   De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.
6. Gerechtvaardigd belang
   De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen, de grondrechten en/of de fundamentele vrijheden van de betrokkene zwaarder wegen dan die gerechtvaardigde belangen. Met name wanneer de betrokkene een kind is, kan dit het geval zijn. Wees zeer terughoudend met het hanteren van deze grondslag.

Bijlage 3: Wanneer mogen bijzondere persoonsgegevens worden vastgelegd?

Verwerking van bijzondere persoonsgegevens (uitgezonderd de strafrechtelijke) is onder de AVG verboden, tenzij sprake is van een van de volgende wettelijke uitzonderingen:

1. Uitdrukkelijke toestemming:
   De betrokkene heeft uitdrukkelijk toestemming gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden.
2. Noodzakelijk uitvoering verplichtingen en uitoefening specifieke rechten:
   De verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten van de verwerkingsverantwoordelijke of de betrokkene op het gebied van het arbeidsrecht en het sociale zekerheids- en sociale beschermingsrecht.
3. Bescherming vitale belangen:
   De verwerking is noodzakelijk ter bescherming van de vitale belangen van de betrokkene of vaneen andere natuurlijke persoon indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven.
4. Verwerking door stichting en vereniging op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied:
   Mits de verwerking uitsluitend betrekking heeft op de leden of de voormalige leden van de instantie of op personen die in verband met haar doeleinden regelmatig contact met haar onderhouden, en de persoonsgegevens niet zonder de toestemming van de betrokkenen buiten die instantie worden verstrekt.
5. Kennelijk openbaar gemaakt door betrokkene:
   De verwerking heeft betrekking op persoonsgegevens die door de betrokkene openbaar zijn gemaakt. De werking moet ook in lijn zijn met het doel van de openbaarmaking door de betrokkene.
6. Noodzakelijk voor rechtsvordering/rechtshandhaving:
   De verwerking is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering of wanneer gerechtsprekende instanties handelen in het kader van hun rechtsbevoegdheid.
7. Zwaarwegend algemeen belang:
   De verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene.
8. Noodzakelijk voor (arbeids)geneeskunde en sociale diensten:
   De verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, op grond van Unierecht of lidstatelijk recht, of uit hoofde van een overeenkomst met een gezondheidswerker en wanneer die gegevens worden verwerkt door of onder de verantwoordelijkheid van een beroepsbeoefenaar die krachtens Unierecht of lidstatelijk recht of krachtens door nationale bevoegde instanties vastgestelde regels aan het beroepsgeheim is gebonden, of door een andere persoon die eveneens krachtens

Unierecht of lidstatelijk recht of krachtens door nationale bevoegde instanties vastgestelde regels tot geheimhouding is gehouden.

9. Noodzakelijk voor algemeen belang volksgezondheid:
   De verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid, zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid of het waarborgen van hoge normen inzake kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen, op grond van Unierecht of lidstatelijk recht waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim.
10. Noodzakelijk voor archivering in het algemeen belang:
    De verwerking is noodzakelijk met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig AVG artikel 89, lid 1, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de belangen van de betrokkene.

    De lidstaten kunnen bijkomende voorwaarden, waaronder beperkingen, met betrekking tot de verwerking van genetische gegevens, biometrische gegevens of gegevens over gezondheid handhaven of invoeren.

Bijlage 4: Het verwerkingsregister

Het Verwerkingsregister moet in ieder geval de volgende gegevens per verwerkingsactiviteit bevatten:

1. Naam en contactgegevens van:
   - uw organisatie, of de vertegenwoordiger van uw organisatie;
   - eventuele andere organisaties met wie u gezamenlijk de doelen en middelen van de verwerking heeft vastgesteld;
   - de Functionaris voor de gegevensbescherming als u die heeft aangesteld;
   - eventuele andere internationale organisaties waar u persoonsgegevens mee deelt.
2. Verwerkingsdoeleinden:
   Beschrijf waarom het persoonsgegeven of de set van persoonsgegevens wordt verwerkt. Persoonsgegevens mogen namelijk alleen verzameld worden voor, zoals de wet het stelt, een 'welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel'. Voorbeelden van verwerkingsdoeleinden zijn het beantwoorden van vragen en klachten van klanten en uitbetaling van salaris.
3. De categorieën betrokkenen
   Beschrijf de categorieën van de personen van wie u gegevens verwerkt, bijvoorbeeld: leden, relaties, potentiële leden, medewerkers van leden en relaties, eigen personeelsleden, uitzendkrachten, klanten, website-bezoekers, leveranciers, mensen die zich hebben aangemeld voor een nieuwsbrief etc.
4. De categorieën van persoonsgegevens
   Bijvoorbeeld: NAW-gegevens van de persoon, bankrekeningnummer, online bestelgeschiedenis of polisnummers. Bepaal of onder deze verwerkte persoonsgegevens zich ook bijzondere persoonsgegevens bevinden en markeer deze. Voor bijzondere gegevens gelden namelijk afwijkende regels en eisen.
5. De (voorgenomen) categorieën van ontvangers van de persoonsgegevens:
   Beschrijf de (voorgenomen) categorieën van ontvangers van de persoonsgegevens zoals de Belastingdienst, Arbodienst of een reclamebureau.
6. Uitvoer naar 3e landen
   Vermeld het derde land of de internationale organisatie waaraan de persoonsgegevens verstrekt (zullen) worden en waar nodig documentatie omtrent de genomen passende waarborgen voor de bescherming van persoonsgegevens in dit derde land.
   Van uitvoer naar een 3e land is sprake wanneer gegevens worden verwerkt buiten de Europese Unie, Noorwegen, Liechtenstein en IJsland. Is er sprake van uitvoer naar 3e landen, onderzoek dan of er voldoende wettelijke waarborgen zijn die uitvoer toestaan.
7. Bewaartermijnen:
   De beoogde bewaartermijnen voor de verschillende categorieën van gegevens.
8. Beveiliging
   Algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Bijlage: 5 Privacyverklaring

De verwerkingsverantwoordelijke moet de betrokkene in duidelijke en eenvoudige taal, bijvoorbeeld in een privacyverklaring, in ieder geval het volgende laten weten:

1. Identiteit van de verwerkingsverantwoordelijke:
   Vermelding van de NAW gegevens van de organisatie.
2. Contactgegevens:
   Hoe kan een persoon contact opnemen met de verwerkingsverantwoordelijke? En indien van toepassing: wat zijn de contactgegevens van de Functionaris voor de Gegevensbescherming? (website, algemeen telefoonnummer, e-mailadres etc.).
3. Geef aan welke persoonsgegevens worden verwerkt.
   Bijvoorbeeld: Voor- en achternaam, geslacht, geboortedatum, geboorte[plaats, adresgegevens, telefoonnummer, emailadres, banknummer e.d.)
4. Geef aan welke bijzondere en/of gevoelige persoonsgegevens worden verwerkt.
   Bijvoorbeeld ziekteverzuim.
5. Doeleinden en rechtsgrond van de verwerking:
   Waarom worden persoonsgegevens verzameld en waarom mag dat?
   (doelomschrijving, rechtsgrond en onderbouwing daarvan)
6. Wie ontvangen de gegevens?
   Aan wie gaat u de persoonsgegevens verder nog verstrekken?
7. Wel of geen verplichting om gegevens te verstrekken:
   Is de betrokkene verplicht om de gevraagde persoonsgegevens te verstrekken of niet? En wat zijn de gevolgen als hij/zij de persoonsgegevens niet verstrekt?
8. Rechten van de betrokkenen:
   Wijs de betrokkene op zijn rechten. Geef aan hoe de betrokkene kan vragen om inzage, rectificatie, overdraging, beperking of het wissen van persoonsgegevens. Hoe de betrokkene bezwaar kan maken en hoe de betrokkene een eerder verleende toestemming weer kan intrekken.
9. Bewaartermijn:
   Hoe lang worden persoonsgegevens bewaard? Of indien dat niet mogelijk is, de criteria ter bepaling van de bewaartermijn.
10. Verwerking derde landen:
    Als de persoonsgegevens buiten de EU, Noorwegen, Liechtenstein en IJsland verwerkt gaan worden, welke waarborgen zijn er dan getroffen zodat de persoonsgegevens in dat derde land conform de AVG verwerkt worden? (Meestal niet van toepassing).
11. Vermelding geautomatiseerde gegevensverzameling:
    Vermeld of er geautomatiseerde besluitvorming (bijvoorbeeld profiling) plaatsvindt.
12. Cookies: Geef duidelijk aan of u gebruik maakt van cookies.
13. Klacht indienen:
    Vermeld hoe de betrokkene een klacht over de privacy kan indienen bij de Autoriteit Persoonsgegevens.

Op de website van veiliginternetten.nl staat een privacyverklaring generator.
https://veiliginternetten.nl/privacyverklaring/

Bijlage 6: Instructie gegevensbeveiliging voor medewerkers.

Door het nemen van de juiste beveiligingsmaatregelen en het in acht nemen van de juiste beveiligingsprocedures willen we voorkomen dat onbevoegden toegang krijgen tot onze bedrijfssystemen, onze vertrouwelijke informatie en de persoonsgegevens die wij beheren.

Werk gerelateerde gegevensverwerking mag alleen worden uitgevoerd met door de werkgever ter beschikking gestelde gegevensdragers, tenzij anders overeengekomen met de directie.
Computers, laptops en tablets:

1. Beveilig de toegang tot je computers, laptops en tablets met een sterk en uniek wachtwoord.
2. Stel multifactor authenticatie in (bijvoorbeeld wachtwoord en daarna pincode)
3. Stel de schermbeveiliging in op maximaal 5 minuten.
4. Installeer in afstemming met de systeembeheerder betrouwbare antivirus-software en houd deze up-to-date.
5. Stel in afstemming met de systeembeheerder een firewall in en houd deze up-to-date.
6. Ga alleen online via een beveiligde verbinding.
7. Stel de automatische update-functie in om besturingssystemen en andere software up-to-date te houden.
8. Download alleen na toestemming van de systeembeheerder nieuwe software en apps.

Losse externe dataopslagapparatuur
Voorbeelden van externe dataopslagapparatuur zijn USB-sticks, externe harde schijven, geheugenkaartjes en cd's/dvd's/blu-ray-discs.

1. Beveilig de toegang tot de losse dataopslagapparatuur met een sterk en uniek wachtwoord.
2. Beveilig de toegang tot de individuele documenten op de losse dataopslagapparatuur met een sterk en uniek wachtwoord.
3. Verwijder na gebruik gegevens van de losse dataopslagapparatuur.

Smartphone

1. Beveilig de toegang tot je telefoon met een pincode van minimaal 4 cijfers.
2. Stel in dat je telefoon automatisch wordt geleegd na 10 verkeerde pincode pogingen.
3. Stel 'zoek mijn iPhone/Android' in en test of dit werkt.
4. Download alleen apps uit de officiële appstores: App-store, Google Play en Windows-store.

Fysieke documenten

1. Voorzie documenten met vertrouwelijke informatie of persoonsgegevens van een duidelijk predicaat 'vertrouwelijk'.
2. Berg fysieke documenten met vertrouwelijke informatie of persoonsgegevens op in een afsluitbare opslagruimte en zorg dat alleen bevoegden toegang hebben tot deze fysieke documenten.

Bijlage 7: Voorbeeld afhandeling recht op inzage

1. **Bepaal wie het verzoek behandeld**
   Beleg in de organisatie wie een inzageverzoek behandelt. Leg dit vast in de procedure of in het register van de verwerkingsactiviteiten.
2. **Voer een identiteitscontrole uit**
   Leg vast hoe de identiteit van de aanvrager wordt gecontroleerd. Stel in dat deze controle altijd wordt uitgevoerd voordat het verzoek verder in behandeling genomen wordt. Deze check moet zwaarder zijn naarmate het om meer gevoelige of zelfs bijzondere gegevens gaat. Voorkomen moet worden dat er een 'fake'-inzageverzoek gedaan wordt om zo gegevens te verzamelen.
3. **Bepaal welke gegevens verstrekt moeten worden**
   De betrokkene heeft het recht om van de verwerkingsverantwoordelijke uitsluitsel te krijgen over:
   - of de organisatie zijn/haar persoonsgegevens gebruikt, en zo ja:
   - om welke gegevens het gaat;
   - wat het doel is van de verwerking;
   - aan wie de organisatie de gegevens eventueel heeft verstrekt (bij uitvoer 3e landen: welke waarborgen);
   - wat de herkomst is van de gegevens, als deze bekend is;
   - het bestaan van geautomatiseerde besluitvorming, profilering en eventueel, informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen;
   - bewaartermijnen.

   De AVG stelt verder dat de betrokkene bij de beantwoording ook gelijk geïnformeerd moet worden over het recht op rectificatie, wissen of beperking van de verwerking en over het feit dat de verzoeker een bezwaar of klacht kan indienen.

   Indien er gegevens van derde personen in de te verstrekken gegevens opgenomen zijn, moet met het (privacy-)belang van die derde rekening gehouden worden. Die gegevens moeten dus of verwijderd worden, of pas na toestemming van die derde verstrekt worden. Denk bijvoorbeeld aan (interne) aantekeningen van een medewerker in een dossier van een lid. Die mogen niet zomaar verstrekt worden.

4. **Verstrek de gegevens aan de betrokkene**
   De verwerkingsverantwoordelijke is verplicht binnen 4 weken schriftelijk of per e-mail te reageren op het inzageverzoek. De AVG stelt geen eisen aan de manier waarop inzage wordt gegeven, maar schrijft wel voor dat de organisatie de verzoeker een kopie verstrekt van de persoonsgegevens die worden verwerkt.
   Onder de AVG moet een kopie van de verwerkte persoonsgegevens kosteloos worden verstrekt en mag alleen voor bijkomende kopieën op basis van de administratieve kosten een redelijke vergoeding in rekening worden gebracht.
   Een inzageverzoek kan geweigerd worden indien dat noodzakelijk is voor de bescherming van de betrokkene of van de rechten en vrijheden van anderen.

Bijlage 8: Voorbeeld afhandeling recht op bezwaar:

1. **Bepaal wie het bezwaar behandeld**
   Beleg in de organisatie wie een bezwaar wegens een specifieke situatie behandelt. Leg dit vast in de procedure of in het register van de verwerkingsactiviteiten.
2. **Voer een identiteitscontrole uit**
   Leg vast hoe de identiteit van de bezwaarmaker wordt gecontroleerd.
3. **Beoordeel het bezwaar**
   Weeg af of het bezwaar redenen bevat om de verwerking van persoonsgegevens van de betrokkene te wijzigen. De verwerkingsgrond speelt een grote rol bij deze beoordeling.
4. **Informeer de betrokkene**
   Informeer de betrokkene schriftelijk of per e-mail binnen 4 weken na ontvangst van het bezwaar of het bezwaar is ingewilligd, hoe dat is gedaan en zo niet, motiveer waarom niet.

Bijlage 9: Voorbeeld afhandeling recht op gegevenswissing

1. **Bepaal wie het verzoek behandeld**
   Beleg in de organisatie wie een gegevenswissingsverzoek behandelt. Leg dit vast in de procedure of in het register van de verwerkingsactiviteiten.
2. **Voer een identiteitscontrole uit**
   Leg vast hoe de identiteit van de aanvrager wordt gecontroleerd. Stel in dat deze controle altijd wordt uitgevoerd voordat het verzoek verder in behandeling genomen wordt. Deze check moet zwaarder zijn naarmate het om meer gevoelige of zelfs bijzondere gegevens gaat. Voorkomen moet worden dat er een 'fake'-wissingsverzoek gedaan wordt om zo gegevens te verwijderen.
3. **Beoordeel en verwerk het verzoek**
   Beoordeel of en hoe aan het verzoek om te wissen kan worden voldaan. Het wissen moet zonder onredelijke vertraging worden gedaan als er geen verwerkingsgrond of geen doelbinding meer is voor de verwerking.
4. Informeer de betrokkene
   Informeer de betrokkene schriftelijk of per e-mail binnen 4 weken na ontvangst van het verzoek of het verzoek is ingewilligd, hoe dat is gedaan en zo niet, motiveer waarom niet.
5. Informeer ontvangers over de wissing
   Informeer ontvangers van de persoonsgegevens over de wissing en zorg dat ook zij de gegevens wissen. Hiervan kan worden afgezien wanneer de ontvangers onmogelijk kunnen worden opgespoord of wanneer het informeren een onevenredige inspanning is.
   Als de gegevens openbaar gemaakt waren, moet de verwerkingsverantwoordelijke zijn best doen ervoor te zorgen dat koppelingen naar derden of kopieën bij derden ook verwijderd worden.

Bijlage 10: Definities

Betrokkenen:
De betrokkene is degene van wie de organisatie persoonsgegevens verwerkt. Dit is dus degene op wie de persoonsgegevens betrekking hebben.

Persoonsgegevens:
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"). Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Bijzondere persoonsgegevens:
Gegevens over iemands:
- gezondheid, inclusief genetische en biometrische gegevens gericht op unieke identificatie van een persoon
- ras of etnische afkomst
- seksueel gedrag of seksuele gerichtheid
- religieuze of levensbeschouwelijke overtuigingen
- lidmaatschap van een vakbond
- politieke opvattingen
- strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen

Een foto van een persoon is alleen een bijzonder persoonsgegeven wanneer de foto met behulp van bepaalde technische middelen wordt verwerkt en zo unieke identificatie van een persoon mogelijk maakt. Soms kan er ook sprake zijn van indirecte bijzondere persoonsgegevens. Dit is het geval wanneer de aanwezigheid van een gevoelig gegeven kan worden afgeleid. Denk hierbij aan de administratie van een kerkgenootschap of een politieke partij.

Volgens de Wpb is het burgerservicenummer (BSN-nummer) ook een bijzonder persoonsgegeven, in de AVG niet.

Verwerking:
Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Verwerker:
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van een verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Verwerkingsverantwoordelijke:
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Profiling:
Elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Bijlage 11: Voorbeeld overzicht gegevensbestanden

1. Inventariseer welke bestanden er binnen de organisatie zijn.
Het gaat zowel om papieren bestanden als om elektronische bestanden.
Bijvoorbeeld personeelsbestand; klantenbestand; relatiebestand, websitebezoeker, leveranciers, ontvangers nieuwsbrief, ledenbestand, bestand potentiële leden etc.

2. Geef per bestand aan welke gewone persoonsgegevens geregistreerd worden.
Bijvoorbeeld NAW-gegevens, geboortedatum, geboorteplaats, e-mailadres, bankrekeningnummer etc.

3. Geef per bestand aan welke bijzondere persoonsgegevens geregistreerd worden.
Bijzondere persoonsgegevens zijn: gegevens over gezondheid, etnische afkomst, geaardheid, levensbeschouwing, vakbondslidmaatschap, politieke opvatting, strafbare feiten of veroordeling of daarmee verband houdende veiligheidsmaatregelen.

4. Geef per bestand aan waarom de gegevens worden geregistreerd
Bijvoorbeeld: afhandelen betaling, verzenden nieuwsbrief, salarisbetaling, belastingaangifte, afleveren van goederen en/of diensten, aanmaken van een account op de website, verlenen van service, toesturen van verenigingsstukken, toesturen van informatie.

5. Geef per bestand aan wat de grondslag voor registratie is.
Gewone persoonsgegevens mogen alleen worden verwerken op basis van een wettelijke grondslag. Dat zijn: toestemming, een wettelijke verplichting, een overeenkomst, het algemeen belang, een vitaal belang of een gerechtvaardigd belang.

Bijzondere persoonsgegevens mogen alleen worden verwerkt als een van deze gronden van toepassing is: Toestemming; noodzakelijke verwerking vanwege verplichtingen uit het arbeidsrecht of sociale zekerheidsrecht; noodzakelijk vanwege preventieve geneeskundige doeleinden, beoordeling arbeidsgeschiktheid werknemer; algemeen belang gezondheidszorg; noodzakelijk voor rechtsvordering; door de persoon zelf openbaar gemaakte gegevens; bescherming vitale belangen; verwerking door kerk of vakbond; zwaarwegend algemeen belang; noodzakelijk voor archivering in kader algemeen belang).

6. Geef per bestand aan wat de bewaartermijn is.
Bij personeelsbestand: altijd; Bij nieuwsbrieven bijvoorbeeld tot melding. Bij levering, zolang nodig is vanuit de belastingen. Alles altijd bewaren is geen optie. Het mag niet langer dan strikt noodzakelijk is.

7. Geef per bestand aan met welke organisaties de gegevens worden gedeeld en waarom.
Personeelsgegevens worden bijvoorbeeld gedeeld met belastingdienst, pensioenfonds, verzekeringsmaatschappij, maar ook bijv. met bedrijven binnen een concern.
Klantengegevens kunnen bijvoorbeeld worden gedeeld met serviceverleners, koeriers, banken.
Als gegevensbestanden worden gedeeld met organisaties in derde landen dan moet dat worden vermeld.

Bijlage 12: Mogelijke inhoud van afspraken met externe verwerkers.

De externe verwerker en de verwerkingsverantwoordelijke zijn verplicht om over zaken rondom de verwerking van persoonsgegevens schriftelijke afspraken te maken. Deze afspraken kunnen in een aparte Verwerkersovereenkomst worden vastgelegd, maar ook onderdeel uitmaken van een andere overeenkomst zoals de leveringsvoorwaarden of de Service Level Agreement (SLA).

Over de volgende aspecten moeten schriftelijke afspraken worden gemaakt:

- Algemene beschrijving
  Een omschrijving van het onderwerp, de duur, de aard en het doel van de verwerking, het soort persoonsgegevens, de categorieën van betrokkenen en de rechten en verplichtingen van de verwerkingsverantwoordelijke.

- Verwerkingsinstructies
  Hoe worden verwerkingsinstructies gegeven en voor welke doeleinden mogen de gegevens worden gebruikt?

- Geheimhoudingsplicht
  Welke geheimhouding is voor wie vereist?

- Beveiliging
  Welke passende beveiligingsmaatregelen worden genomen?
  Wat te doen bij datalekken.

- Subverwerkers
  Hoe worden eventuele subverwerkers ingeschakeld? Is toestemming nodig?

- Privacyrechten
  Op welke wijze helpt de verwerker de verwerkingsverantwoordelijke om aan zijn plichten te voldoen als betrokkenen hun privacyrechten uitoefenen?

- Aansprakelijkheid tussen partijen.

- Andere verplichtingen
  Op welke wijze helpt de verwerker de verwerkingsverantwoordelijke ook om andere verplichtingen na te komen, zoals bij het melden van datalekken, het uitvoeren van een DPIA en bij een voorafgaande raadpleging.

- Gegevens verwijderen
  Welke handelswijze wordt gehanteerd na afloop van de verwerkingsdiensten?

- Controle door de verwerkingsverantwoordelijke.
  Hoe wordt naleving van deze overeenkomst gecontroleerd?