



# Wat zijn AVG/GDPR vereisten voor vrijwilligersmanagementsoftware in Nederland?

Inclusief specifieke overwegingen voor verwerking vrijwilligersdata, consent management, data retentie, en recht op vergetelheid. Focus op praktische implementatie voor kleine tech bedrijven in Nederland.

Now I'll create the comprehensive report for the user.

## AVG/GDPR Vereisten voor Vrijwilligersmanagementsoftware in Nederland

### Samenvatting

Als softwarebedrijf dat vrijwilligersmanagementsoftware aanbiedt, bent u in GDPR-termen de **data processor** – u verwerkt persoonsgegevens namens uw klanten (de controllers). Dit brengt specifieke verplichtingen mee die essentieel zijn voor rechtmatige bedrijfsvoering. Deze rapportage biedt een praktisch raamwerk voor implementatie in kleine technologiebedrijven.

### 1. Kernverantwoordelijkheden van Uw Rol als Processor

#### 1.1 Controller vs. Processor

In het GDPR-kader staat duidelijk vastgesteld: Uw organisatie als softwareleverancier fungeert als **data processor**—u verwerkt persoonsgegevens uitsluitend op instructie van de organisatie (de data controller) die uw software gebruikt. Dit verschil is kritiek omdat het bepaalt wie aansprakelijk is voor wat.<sup>[1]</sup>

Aspect	Controller (Vrijwilligersorganisatie)	Processor (Uw Softwarebedrijf)
<b>Wie bepaalt waarom &amp; hoe?</b>	Controller (doeleinde en middelen)	Volgt controller-instructies alleen
<b>Contractuele verplichting</b>	Bepaalt verwerkingsdoel	Mag geen eigen doeleinden toevoegen
<b>Aansprakelijkheid</b>	Primair aansprakelijk voor AVG-compliance	Aansprakelijk voor beveiging en instructie-naleving
<b>Recht op audits</b>	Kan audits uitvoeren	Moet audittoegang verlenen

**Praktische implicatie:** U kunt niet zelf bepalen "we gaan deze gegevens gebruiken voor marketing" of "we delen met derden." Alles wat u doet moet binnen de grenzen van de controller's instructies blijven, vastgelegd in een verwerkersovereenkomst.

## 1.2 Verwerkersovereenkomst (Data Processing Agreement) – Verplicht

Artikel 28(3) van het GDPR maakt duidelijk: beide partijen zijn in overtreding zonder een geschreven verwerkersovereenkomst. Dit is niet optioneel.<sup>[2]</sup>

**Wat moet erin:**

- Onderwerp, aard, duur, doel en plaats van verwerking
- Categorieën betrokkenen (b.v. "vrijwilligers, organisatiemedewerkers")
- Soort persoonsgegevens ("naam, e-mail, telefoonnummer, functie")
- Veiligheidsmaatregelen die u implementeert
- Recht van controller op audits en inspecties
- Sub-processor afspraken (zie sectie 3)
- Procedure bij datalek
- Exit-procedures (data teruggeven/vernietigen bij stopzetting)
- Vertrouwelijkheid van medewerkers

**Praktische tip:** Gebruik een template. De Autoriteit Persoonsgegevens publiceert richtlijnen, en organisaties als ICT Institute en SoftwareZaken bieden gratis templates. Pas deze aan voor uw specifieke software.<sup>[3]</sup>

## 2. Gegevensverwerkingsgrondslagen & Toestemmingsmanagement

### 2.1 Rechtsgrondslagen voor Vrijwilligersgegevens

Uw klanten (controllers) moeten één van zes wettelijke grondslagen hebben om persoonsgegevens te verwerken. Voor vrijwilligerswerk zijn de meest relevant:<sup>[4]</sup>

#### Grondslag 1: Contractueel Noodzakelijk (Artikel 6(1)(b))

Dit is de primaire grondslag voor vrijwilligers. Gegevens die nodig zijn voor:

- Registratie en identificatie van vrijwilligers
- Taakering en inschedeling
- Communicatie over opdrachten
- Noodcontactinformatie

Geen toestemming nodig—deze gegevens zijn simpelweg noodzakelijk.

#### Grondslag 2: Wettelijke Verplichting (Artikel 6(1)(c))

- BSN voor belastingdoeleinden

- Verplichte verificaties (bijvoorbeeld VOG-antecedenten)
- Arbeidsgezondheidsinformatie indien verplicht

### **Grondslag 3: Gerechtvaardigd Belang (Artikel 6(1)(f))**

Alleen voor zeer specifieke doelen met duidelijke afweging:

- Fraudebestrijding
- Veiligheid van vrijwilligers en begunstigden
- Juridische verdediging (bij geschillen)

Uw klanten moeten deze afweging documenteren—u moet deze begeleiding in uw software en documentatie verduidelijken.

### **Grondslag 4: Toestemming (Artikel 6(1)(a))**

Voor niet-contractuele verwerking:

- Marketing of nieuwsbrieven
- Foto's publiceren
- Gegevens delen met partners

**Kritieke implementatie:** Uw software moet controllers helpen duidelijk de rechtsgrondslagen vast te stellen en deze transparant te communiceren naar vrijwilligers.

## **2.2 Toestemmingsmanagement (Consent Management)**

Voor toestemming gelden strikte vereisten:<sup>[5]</sup> <sup>[6]</sup>

- **Vrijwillig:** Geen dwang of manipulatie (geen vooraf aangevinkte vakjes)
- **Specifiek:** Toestemming voor elke verschillende verwerkingsdoel apart
- **Ondubbelzinnig:** Actieve handeling (een vakje aankruisen, niet "niet-aanvinken als je niet akkoord bent")
- **Geïnformeerd:** Persoon moet begrijpen wat ze toestaan

**In uw software:**

- 1. Expliciete Opt-In Formulieren:** Laat controllers formulieren maken met per doel een aparte checkbox
- 2. Audit Trail:** Registreer automatisch:
  - Wie heeft toestemming gegeven
  - Wanneer (datum/tijd)
  - Voor welke specifieke doeleinden
  - Versie van de privacyverklaring op dat moment
  - IP-adres (aanbevolen voor verificatie)
- 3. Eenvoudige Intrekking:** Vrijwilligers moeten met één klik toestemming kunnen intrekken
- 4. Preference Center:** Laat gebruikers hun voorkeuren op elk moment aanpassen

## **Praktijk voorbeeld:**

- Ik wil geïnformeerd blijven over vrijwilligersmogelijkheden via e-mail
- Ik sta toe dat mijn foto wordt gebruikt in PR-materiaal van de organisatie
- Ik geef toestemming voor verwerking van gezondheidsgegevens (bijv. allergieën)

Niet: "Ik ga akkoord met alle voorwaarden" (te breed).

## **3. Gegevensretentie & Het Recht op Vergetelheid**

### **3.1 Retentieperiodes Bepalen**

Het AVG bepaalt geen vaste wettelijke termijn. Uw klanten moeten zelf bewaartijden vaststellen op basis van het verwerkingsdoel. Voor vrijwilligersgegevens:<sup>[7]</sup>

Gegevenstype	Retentieperiode	Grondslag
Actieve vrijwilliger-gegevens	Zolang actief + 1 maand na stopzetting	Contractueel noodzakelijk
Werkgeversgetuigschriften / References	5 jaar	Arbeidsrecht (geschillen)
Medische/gezondheidsgegevens	Geval-per-geval (vaak 3-5 jaar)	Wettelijk vereist
Bankgegevens voor betaling	Tot 7 jaar (belastingvereiste)	Belastingwet
Contactgegevens na opt-out (marketing)	Direct verwijderen	Intrekking toestemming
Logbestanden / Access logs	Maximaal 12 maanden	Beveiligingsdoeleinden

### **Implementatie in uw software:**

- Laat controllers retentie-instellingen configureren per gegevenstype
- Zet automatische verwijderingskronogrammen in
- Waarschuw voordat gegevens worden verwijderd
- Voer het "soft delete" uit (markeer als verwijderd, bewaar audit trail)

### **3.2 Recht op Vergetelheid (Artikel 17 AVG)**

Individuen kunnen verwijdering eisen onder bepaalde voorwaarden:<sup>[8] [9]</sup>

- Gegevens zijn niet meer nodig voor doel
- Toestemming is ingetrokken (geen ander rechtsbasis)
- Gegevens onrechtmatig verwerkt
- Wettelijke verplichting tot verwijdering
- Betrokkene maakt gegrond bezwaar

**Reactietermijn:** Maximaal 1 maand (extendible met 2 maanden bij complexiteit).

## **Uitzonderingen** (u/uw klant mag weigeren):

- Juridische verplichtingen (b.v. belastingdossiers)
- Verdediging van rechtsgebruiken
- Archivering van openbaar belang
- Medische doeleinden

## **Praktische implementatie:**

**1. Self-Service Portal:** Laat vrijwilligers een verwijderingsverzoek indienen

### **2. Workflow:**

- Verificatie identiteit
- Beoordeling uitzonderingen
- Confirmatie verwijdering
- Documentatie

### **3. Verwijderingsbewerking:**

- Verwijder uit alle actieve databases
- Verwijder uit backups (of wacht tot backups vervallen)
- Verwijder gelinkte documenten
- Update audit logs (niet: verwijder logs zelf)

## **4. Gegevensbescherming & Beveiligingsmaatregelen**

Artikel 32 AVG vereist "passende technische en organisatorische maatregelen." Dit is niet prescriptief maar risico-georiënteerd. Voor vrijwilligerssoftware die gevoelige gegevens verwerkt:<sup>[6]</sup>

### **4.1 Technische Maatregelen**

Maatregel	Implementatie	Waarom
<b>Encryptie in Transit</b>	TLS 1.2+ voor alle API's & downloads	Voorkómen man-in-the-middle aanvallen
<b>Encryptie at Rest</b>	AES-256 voor databases, key management	Voorkómen datalekken bij databasebreuk
<b>Twee-Factor Authenticatie</b>	2FA voor alle admin-accounts verplicht, optioneel voor users	Voorkómen account-takeover
<b>Access Control</b>	Role-based permissions (RBAC): admin, coördinator, vrijwilliger	Beperk wie wat ziet/aanpast
<b>Logging &amp; Monitoring</b>	Elk data-access event loggen (wie, wat, wanneer)	Audit trail & anomaliedetectie
<b>Regelmatige Updates</b>	Security patches binnen 30 dagen	Plug beveiligingsgaten

Maatregel	Implementatie	Waarom
<b>Backup Procedures</b>	Versleutelde backups, off-site opslag, restore-testen	Data recovery zonder gegevens bloot te stellen
<b>Penetratie Testing</b>	Jaarlijkse audit (intern of extern)	Proactief risico's identificeren

## 4.2 Organisatorische Maatregelen

- **Medewerker-Training:** AVG-training bij start en jaarlijks
- **Data Processing Agreement Audit:** Controleer of alle processors hun verplichtingen naleven
- **Incident Response Plan:** Datalekprotocol (zie sectie 5)
- **Sub-processor Review:** Zorg dat sub-contractors dezelfde normen hanteren
- **Privacy by Design:** Zet privacy in vanaf softwareontwikkeling, niet achteraf

## 5. Datalekkenprotocol & Meldplicht

### 5.1 Wat Telt als een Datalek?

Artikel 33 AVG definieert datalekken als "beveiligingsincidenten die verlies, diefstal of ongeautoriseerde inzage van persoonsgegevens veroorzaken." [10] [11]

#### Voorbeelden:

- Database-hack
- Phishing-aanval leidt tot geleakte gegevens
- Backup-apparaat kwijtraakt
- Medewerker verwijdert per ongeluk gegevens
- Niet alle gegevens zijn verwijderd na verwijderingsverzoek

### 5.2 Meldingsprocedure

#### Stap 1: Detectie & Isolatie (direct)

- Identificeer het beveiligingsincident
- Isoleer getroffen systemen
- Zet loggen aan om omvang vast te stellen

#### Stap 2: Beoordeling (binnen 24 uur)

Bepaal of dit meldplichtig is: "Vormt dit waarschijnlijk een risico voor de rechten en vrijheden van betrokkenen?"

Risicofactoren:

- **Aard gegevens:** Identiteitsgegevens + financiële data = hoger risico; anoniem e-mailadres = lager risico
- **Aantal getroffen personen:** 1 persoon = lager; 10.000+ = hoger
- **Gevolgen:** Identiteitsdiefstal mogelijk? Discriminatie? Financiële schade?
- **Of versleuteling werkte:** Versleutelde gegevens zonder sleutels = lagere meldplicht

#### **Uitzonderingen (Geen melding nodig):**

- Versleutelde gegevens en sleutels zijn niet gecompromitteerd
- Gegevens zijn anoniem
- Risico is zeer laag (bijv. eenmalige lezing door onbevoegde intern)

#### **Stap 3: Melding Autoriteit Persoonsgegevens** (binnen 72 uur) [\[11\]](#) [\[10\]](#)

Meld via: <https://www.autoriteitpersoonsgegevens.nl/datalekken-melden>

#### **Inhoud melding:**

- Aard en omvang inbreuk
- Waarschijnlijke gevolgen
- Getroffen categorieën betrokkenen (geschatte aantallen)
- Contactpersoon FG/DPO (of uw contactpersoon)
- Genomen/voorgestelde maatregelen

#### **Stap 4: Betrokkenen Informeren** (zonder onnodige vertraging)

U moet betrokkenen informeren als het risico hoog is TENZIJ:

- Technische beveiligingsmaatregelen (bijv. encryptie) de data onleesbaar maken
- Later berichten uitgewerkt zijn

#### **Inhoud bericht aan betrokkenen:**

- Wat is er gebeurd (begrijpelijke uitleg, geen technojargon)
- Welke gegevens zijn getroffen
- Wat zijn mogelijke gevolgen
- Wat kunnen zij doen (wachtwoord resetten, monitoring activeren)
- Contact voor vragen

### **5.3 Datalekkenregister Onderhouden**

Houd een register bij (ook niet-gemelde datalekken):

Incident	Datum	Omvang	Oorzaak	Meldplicht	Status
Verloren USB-stick	15-11-2024	50 personen	Medewerker slordighheid	Nee (versleuteld)	Gesloten

Incident	Datum	Omvang	Oorzaak	Meldplicht	Status
Database hack poging	20-11-2024	0	Brute force	Nee (mislukt)	Gesloten
Fout mailbericht	25-11-2024	200 personen	Verkeerd e-mailadres	Ja	Gemeld, betrokkenen geïnformeerd

## 6. Data Protection Impact Assessment (DPIA) – Wanneer Nodig?

Een DPIA is een risicoanalyse voordat u een nieuwe verwerkingsactiviteit begint. [12] [13] [14]

### 6.1 Wanneer Verplicht?

De meeste vrijwilligerssoftware heeft **geen DPIA nodig**, BEHALVE als u:

- **Bijzondere persoonsgegevens op grote schaal verwerkt** (artikel 9: gezondheid, religie, biometrisch)
- **Geautomatiseerde profiling** implementeert (bijv. "aanbeveel vrijwilliger X voor taak Y")
- **Cameratoezicht** of tracking
- **Gegevens van kwetsbare groepen** (kinderen, mentaal onbekwame personen)

Voor vrijwilligerssoftware relevante scenario's:

- Software voor zorgorganisaties die gezondheidsgegevens verwerkt → DPIA
- Matchingalgoritme dat automatisch vrijwilligers aanbeveelt → DPIA
- Basisadministratie (naam, e-mail, telefoonnummer) → Geen DPIA

### 6.2 DPIA Uitvoering

Mag zelf gedaan worden; geen externe expert nodig voor kleine bedrijven.

**Stappen:**

1. Beschrijf gegevensverwerking in detail
2. Identificeer privacyrisico's
3. Beoordeel waarschijnlijkheid & ernst risico's
4. Definieer risicomaatregelen
5. Documenteer bevindingen

## 7. Bijzondere Persoonsgegevens (Artikel 9 AVG)

Veel vrijwilligersorganisaties verwerken gevoelige gegevens. Dit vereist extra zorg.

## **7.1 Wat zijn Bijzondere Gegevens?**

Artikel 9 AVG verbiedt verwerking van:

- **Gezondheidsgegevens:** Fysieke/mentale gezondheid, medische behandeling, diagnose
- **Religie/Levensovertuiging:** Religieuze voorkeur, bezinning
- **Ras/Etnische Herkomst:** (zeer gevoelig, zelden nodig)
- **Biometrisch:** Gezichtsherkenning, vingerafdrukken
- **Seksuele Oriëntatie/Geslacht**
- **Politieke Affiliatie**
- **Strafrechtelijke Veroordelingen**

**Voorbeelden in vrijwilligerswerk:**

- "Deze vrijwilliger mag niet tillen (rugproblemen)" → GEZONDHEID
- "Vervoering nodig; geen auto beschikbaar" → Kan gezondheid impliceren
- "Voorkeur voor organisatie van type X" → Kan religie impliceren

## **7.2 Uitzonderingen Verwerking**

U mag bijzondere gegevens verwerken ALLEEN als:

1. **Expliciete toestemming** gegeven (veel strenger dan normale toestemming) + ÉÉN van:
  - Contractueel noodzakelijk (zeer nauw) + leverancier niet-discriminatie waarborgen
  - Werkgevers- of personeelsdoeleinden (UAVG artikel 30) + waarborgen
  - Bescherming vitaal belang (noodsituatie)
  - Non-profit organisatie (bijv. kerk of bond) + passende waarborgen

**Praktische implicatie:**

- Uw software moet controllers helpen waarborgen dat verwerking van gezondheidsgegevens gerechtvaardigd is
- Sub-processor DPA's moeten stricter zijn (gezondheidsgegevens + DPA-vereisten)
- Mogelijk DPIA verplicht

## **8. Specifieke Praktische Implementatie voor Uw Softwarebedrijf**

### **8.1 Fase 1: Audit & Planning (Weken 1-2)**

**Week 1: Gegevensinventaris**

- Welke gegevens verwerkt uw platform (actueel)?
- Categorieën betrokkenen (vrijwilligers, organisatiemedewerkers, begunstigden)?
- Verwerking locaties (EU datacenters? Sub-processors?)

#### **Checklist:**

- Inventaris persoonsgegevens opgesteld
- Verwerkingsdoeleinden per gegevenstype gedefinieerd
- Retentierijmijnen per type bepaald
- Rechtsgrondslagen geïdentificeerd
- Sub-processors gelabelleerd

## **8.2 Fase 2: Contracten & Documentatie (Weken 2-4)**

#### **Verwerkersovereenkomst (DPA)**

- Gebruik template (bijv. ICT Institute)
- Pas aan voor uw service
- Laat klanten deze ondertekenen vóór data-access

#### **Privacy Beleid & Transparantie**

- Beschrijf hoe u data verwerkt
- Welke sub-processors gebruikt u (bijv. Microsoft Azure)
- Hoe lang bewaart u backups
- Wie heeft access (uw medewerkers? Support?)

#### **Verwerkersregister**

- Een lijstje van alle verwerkingsactiviteiten
- Voor kleine bedrijven eenvoudig:

Activiteit	Gegevenstypes	Betrokkenen	Rechtsbasis	DPA aanwezig?
Vrijwilliger-registratie	Naam, e-mail, tel., adres	Vrijwilligers	Contractueel	Ja
Loggen systeemtoegang	User ID, timestamp, action	Organisatiemedewerkers	Gerechtvaardigd belang	Ja

## **8.3 Fase 3: Technische Maatregelen (Lopend)**

#### **Checklist Beveiliging:**

- TLS 1.2+ op alle endpoints
- AES-256 database-encryptie
- Backups versleuteld
- 2FA ingeschakeld (admin)
- Role-based access control (RBAC)

- Logging van data-toegang
- Regelingen voor updates (maandelijks minimum)
- Incident response plan
- Penetratie testing (jaarlijks)

## 8.4 Fase 4: Operationele Processen (Continuo)

### Medewerkerstraining

- AVG-training verplicht voor iedereen die data aanraakt
- Jaarlijks herhalen
- Deel aan korte modules (niet: 8-uur sessie)

### Verzoekmanagement

- Inzageverzoeken (copy van hun data) → 30 dagen termijn
- Correctieverzoeken → 30 dagen
- Verwijderingsverzoeken → 30 dagen (met uitzonderingen)

### Incident Protocol

- Wie rapporteert datalek? (Medewerker → Manager → CISO/DPO)
- Wie beoordeelt meldplicht?
- Wie meldt bij AP?
- Sjabloon voor betrokkenen-notificatie

### Jaarlijks Review

- Zijn uw sub-processors nog AVG-compliant?
- Zijn uw retentieperiodes nog redelijk?
- Zijn er klachten geweest?
- Zijn er wettelijke veranderingen?

## 9. Sub-Processor Afspraken & Cloud Afhankelijkheden

### 9.1 Sub-Processor Keten

Veel SaaS-bedrijven gebruiken cloud providers. Deze zijn sub-processors.<sup>[15]</sup> <sup>[16]</sup>

**Voorbeeld:** Uw software draait op Microsoft Azure (sub-processor). Dit vereist:

1. Uw DPA met klanten moet sub-processors noemen
2. Klanten moeten op de hoogte zijn van wijzigingen
3. Azure moet dezelfde beschermingen bieden als u

## **Veelvoorkomende Sub-processors in software:**

- **Cloud compute:** Microsoft Azure, AWS, Google Cloud
- **Email:** SendGrid, Mailgun
- **Payments:** Stripe, Adyen
- **Analytics:** Mixpanel (indien gebruikt)
- **Monitoring:** Datadog, New Relic

## **Voor elk:**

- Controleer hun DPA
- Zorg dat zij GDPR-compliant zijn
- Voeg toe aan uw "Sub-processor Liste"
- Bel klanten in kennis indien wijzigingen

## **9.2 EU-US Datatransfers (Schrems II)**

Is uw data op US-servers? Dit brengt extra vereisten:

- Standaard Contractuele Clauses (SCC's) verplicht
- Additionele beschermingsmaatregelen
- Mogelijk extra DPA-bepalingen

Veel cloud providers bieden dit; vraag hun DPA.

## **10. Toepasbare Retentieperiodes per Gegevenstype (Richtlijn)**

Uw klanten moeten deze zelf bepalen, maar richt hen:

Gegevenstype	Retentie	Opmerking
<b>Actieve vrijwilliger-basis</b>	Zolang actief + 1 maand	Contractueel noodzakelijk
<b>Werkgeversgetuigschrift</b>	5 jaar	Arbeidsgeschillen
<b>Gezondheidsgegevens</b>	3-5 jaar (geval-afhankelijk)	Consult wettelijk adviseur
<b>Nood-contactgegevens</b>	Zolang relatie actief	Contractueel
<b>Foto's/PR-materiaal</b>	Geldende toestemming termijn	Zolang toestemming geldig
<b>Bankgegevens (betaling)</b>	7 jaar	Belastingwet
<b>Server logs / Access logs</b>	12 maanden	Beveiligingsdoeleinden
<b>Backed-up data</b>	Standaard backup-cyclus (b.v. 30 dagen)	Maar verwijderde data kan achterblijven
<b>Opt-out contacten</b>	Direct verwijderen	Niet opslaan na opt-out

## 11. Templates & Gereedschappen

### Gratis Beschikbare Templates Nederlands

Template	Bron	Geschikt voor
Verwerkersovereenkomst	ICT Institute / SoftwareZaken	DPA voor alle SaaS
Privacy Beleid	<a href="#">PrivacyPolicies.com</a> / Autoriteit PG	Website/app
Vrijwilligersovereenkomst	NOV / VrijwilligersCentrale	Uitbreiden met gegevensbijlage
Datalekkenprotocol	Diverse; zie Autoriteit PG site	Intern incident response
DPIA Template	Autoriteit Persoonsgegevens	Risicoanalyse indien nodig

### Online Hulpmiddelen

Tool	Functie	Kosten
<a href="#">AVG-support.nl</a>	Gratis checklist & stappenplan	Gratis / €40/jaar premium
Autoriteit Persoonsgegevens ( <a href="#">www.autoriteitpersoonsgegevens.nl</a> )	Officiële richtlijnen, templates, meldformulier	Gratis
<a href="#">GDPR-info.eu</a>	Interactieve gids door alle artikelen	Gratis
Privacy Audit Tools	Bijv. TermsFeed, iubenda	Gebaseerd op plan

## 12. Risico's & Boetes

De AVG enforceert serieus. Boetes voor non-compliance:

Severity	Boete	Voorbeelden
<b>Basis (artikel 15-22, etc.)</b>	Tot €10 miljoen OF 2% globale omzet	Geen DPA, geheime verwerking, geen inzage
<b>Ernstig (artikel 5-8, 32-36)</b>	Tot €20 miljoen OF 4% globale omzet	Datalek zonder meldplicht, geen toestemming, slechte beveiliging

### Voor kleine bedrijven:

- Veel ondernemingen krijgen waarschuwingen voordat boetes
- Maar herhaalde overtredingen → stijgende boetes
- Reputatieschade (publieke lijsten van boetes)
- Klanten kunnen vragen DPA op te zeggen

**Actuele handhaving:** De Autoriteit Persoonsgegevens publiceert alle handhavingsacties. Veel kleine bedrijven krijgen waarschuwingen en adviezen—zorg dat u niet in de openbare "boetelijst" terechtkomt.

## 13. Praktische Stappenplan (90 Dagen)

### Maand 1: Voorbereiding

- Week 1: Audit huidige praktijken
- Week 2: Gegevensinventaris opstellen
- Week 3: DPA-template aanpassen en intern goedkeuren
- Week 4: Klanten contacteren met DPA's ter ondertekening

### Maand 2: Documentatie & Training

- Week 5: Privacy Beleid schrijven / updaten
- Week 6: Sub-processor liste vaststellen
- Week 7: Medewerker AVG-training inplannen
- Week 8: Datalekkenprotocol documenteren

### Maand 3: Techniek & Testing

- Week 9: Beveiligingscontroles implementeren (TLS, encryptie, logging)
- Week 10: Verwijderings-workflows testen
- Week 11: Inzage-requests testen
- Week 12: Penetratie test / security audit inplannen (volgende kwartaal)

### Conclusie

AVG/GDPR-compliance voor vrijwilligersmanagementsoftware vereist drie pijlers:

1. **Juridisch:** DPA's, Privacy Beleid, Verwerkersregister
2. **Technisch:** Encryptie, Logging, Beveiligingscontroles
3. **Operationeel:** Trainingen, Incident Response, Sub-processor Oversight

Voor een klein technologiebedrijf hoeft dit niet overweldigend te zijn. Start met een gratis DPA-template, voeg beveiligingsmaatregelen toe, en zet processen in. Het resultaat: vertrouwde klanten, geen boetes, en een defensibele positie bij controles.<sup>[17]</sup> <sup>[18]</sup> <sup>[19]</sup>

De Autoriteit Persoonsgegevens en Nederlandse brancheverenigingen bieden gratis richtlijnen. Maak daar gebruik van voordat u externe juridische adviseurs inhoopt.

### Referenties:

Ledenadministratie Online - GDPR/AVG Vreugd Software als verwerker; Vrijwilligersaanzet - Privacy verklaring; NOV - AVG privacyregels; Vereniging Vrijwilligerswerk - AVG privacyregels; Secure Privacy - GDPR Consent Management; Vooruit - Wat zegt de AVG over data verwijderen; GDPR-info - Right to be Forgotten; Autoriteit Persoonsgegevens - Controller and Processor;

Autoriteit Persoonsgegevens - Bewaren van persoonsgegevens; Autoriteit Persoonsgegevens - Processing Agreement; Kiwa - Data Protection Impact Assessment; De Zaak - Privacyregels voor ondernemers; Vrijwilligersaanzet - Vrijwilligers en de AVG; Werkaanuitvoering - DPIA; Autoriteit PG - Gezondheidsgegevens; Autoriteit PG - DPIA; NTNT Rotterdam - Datalek meldplicht; SoftwareZaken - Template verwerkersovereenkomst; Aucuba - Datalek meldplicht; Sumrin - AVG en arbeidscontracten; DataGuard - Data Controller vs Processor; Free Privacy Policy - Liability data controllers/processors; KPI Solutions - Verwerkersovereenkomst; Autoriteit PG - Grondslagen AVG uitgelegd. [20] [18] [19] [9] [21] [13] [22] [14] [23] [24] [16] [17] [5] [8] [1] [7] [2] [12] [6] [10] [3] [11] [15] [4]

\*\*

1. <https://www.autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-basics/controller-and-process>
2. <https://www.autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-basics/processing-agreement>
3. <https://softwarezaken.nl/2018/02/gratis-template-verwerkersovereenkomst/>
4. <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/grondslagen-avg-uitgelegd>
5. <https://secureprivacy.ai/blog/gdpr-consent-management>
6. <https://www.dezaak.nl/juridisch/wet-regelgeving/privacyregels-voor-ondernemers-maak-je-bedrijf-avging-proof-in-7-stappen/>
7. <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacy-en-persoonsgegevens/bewaren-van-persoonsgegevens>
8. <https://vooruit.nl/wat-zegt-de-avg-over-data-verwijderen/>
9. <https://gdpr-info.eu/issues/right-to-be-forgotten/>
10. <https://www.ntnt.nl/wat-moet-ik-doen-bij-een-datalek-volgens-avg/>
11. <https://aucuba.nl/kennisbank/uncategorized/wat-moet-ik-doen-bij-een-datalek-volgens-avg/>
12. <https://www.kiwa.com/nl/nl/diensten/certificering/data-protection-impact-assessment-dbia/>
13. <https://www.werkaanuitvoering.nl/onderwerpen/kennisbank/data-protection-impact-assessment-dbia>
14. <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/data-protection-impact-assessment-dbia>
15. <https://www.dataguard.com/blog/data-controllers-and-processors-liability-roles-in-data-protection>
16. <https://kpisolutions.nl/wp-content/uploads/2022/06/06-2022-KPI-Standaard-verwerkersovereenkomst.pdf>
17. <https://ledenadministratieonline.nl/gdpr-avg-vreugd-software-als-verwerker/>
18. <https://vrijwilligerswerk.nl/themas/wettenenregels/wenr-inzicht/2497703.aspx>
19. <https://www.vrijwilligerswerk.nl/kennis/wetten-en-regels/2497703.aspx?t=AVG-privacyregels>
20. <https://www.vrijwilligersaanzet.nl/privacy-verklaring/>
21. <https://www.vrijwilligersaanzet.nl/vrijwilligers-en-avg-zo-bereid/>
22. <https://www.autoriteitpersoonsgegevens.nl/themas/gezondheid/gezondheidsgegevens-gebruiken-en-elen>
23. <https://www.sumrin.nl/stand-van-zaken-nieuwe-avg-wetgeving/>
24. <https://www.freeprivacypolicy.com/blog/liability-data-controllers-processors/>

25. <https://edepot.wur.nl/670109>
26. <https://www.transip.nl/iubenda/consent-management-platform/>
27. <https://zakelijk.nlvoorelkaar.nl/2098-avg-aandachtspunten-voor-vrijwilligerswerk-platformen/>
28. <https://www.vca.nu/de-avg-hoe-ga-je-om-met-persoonlijke-gegevens/>
29. <https://www.involv.nl/kennisbank/10-checks-voor-de-privacywet-avg>
30. <https://complydog.com/blog/right-to-be-forgotten-gdpr-erasure-rights-guide>
31. <https://www.schulinck.nl/opinie/gegevens-bewaren-archiveren-en-vernielenhoe-zit-het-met-de-privacy-4-tips/>
32. <https://gdpr.eu/right-to-be-forgotten/>
33. <https://ictinstitute.nl/wp-content/uploads/2021/02/Template-GDPR-Data-Processing-Agreement.docx>
34. <https://www.avg-support.nl/nieuws/geheimhoudingsverklaringen-en-de-avg/>
35. <https://www.privacypolicies.com/nl/blog/privacybeleid-template/>
36. <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/verantwoordingsplicht>
37. [https://www.lerenwerkenmetdata.nl/assets/uploads/2025\\_1- AVG-en-privacy-rondom-data-in-de-gehandicaptenzorg-deel-1-Met-data-aan-de-slag-wat-moet-je-weten-en-hoe-helpt-de- AVG-hierbij.pdf](https://www.lerenwerkenmetdata.nl/assets/uploads/2025_1- AVG-en-privacy-rondom-data-in-de-gehandicaptenzorg-deel-1-Met-data-aan-de-slag-wat-moet-je-weten-en-hoe-helpt-de- AVG-hierbij.pdf)
38. <https://www.avg-support.nl/nieuws/zelf-avg-regelen-voor-je-vereniging/>
39. [https://www.vrijwilligersaanzet.nl/wp-content/uploads/2019/02/voorbeeld\\_vrijwilligerscontract.pdf](https://www.vrijwilligersaanzet.nl/wp-content/uploads/2019/02/voorbeeld_vrijwilligerscontract.pdf)
40. <https://www.ntnt.nl/moet-ik-alle-datalekken-melden-bij-de-autoriteit-persoonsgegevens/>
41. <https://www.semble.nl/blogs/avg-proof-in-5-stappen-de-semble-privacychecklist-voor-verenigingen/>
42. <https://www.erfgoedvrijwilliger.nl/verdieping/model-vrijwilligersovereenkomst/>
43. <https://aucuba.nl/kennisbank/uncategorized/moet-ik-alle-datalekken-melden-bij-de-autoriteit-persoonsgegevens/>
44. <https://slimmicrosoftrijk.nl/wp-content/uploads/2021/01/factsheet-verwerksovereenkomst.pdf>
45. <https://www.openvoorcultuur.nl/sites/ovc/files/2023-05/20180703-privacyverklaring-werknemers-sollicitanten-vrijwilligers-en-stagiares1.pdf>
46. <https://www.stichtingbuitenzorg.nl/wp-content/uploads/2019/03/AVG-Protocol-Buitenzorg-versie-10-2021.pdf>
47. <https://www.neumetric.com/journal/role-data-processors-gdpr-compliance/>
48. <https://woxow.nl/gegevensverwerkingsovereenkomst/>