Universiteit Utrecht

De AVG in 10 vragen *(en antwoorden)*

Een praktische gids voor studie- en studentenverenigingen

Universiteit Utrecht

Bij de bestuursleden van veel studie- en studentenverenigingen heerst er nogal wat onduidelijkheid over de vraag wat ze met persoonsgegevens mogen doen en wat ze moeten regelen op het gebied van de Algemene verordening gegevensbescherming (AVG). Wat mag wel en wat mag niet? Wat moet wel en wat hoeft niet?

Aan de hand van de antwoorden op een tiental vragen proberen de privacy officers van de Universiteit Utrecht jullie enigszins op weg te helpen. En heb je geen tijd om deze hele brochure door te lezen, stel jezelf dan in ieder geval deze ene vraag: ***Hoe zou je zelf willen én verwachten dat een vereniging met jouw persoonsgegevens zou omgaan?***

Vragen *(en antwoorden)*

1. Wat moeten we als vereniging allemaal regelen?

Veel van de dingen die je moet regelen, worden al in dit document besproken. Hoeveel je moet doen, is ook afhankelijk van de omvang van je vereniging. Van een vereniging met een paar duizend leden wordt echt wel meer verwacht dan van een clubje van slechts een handvol enthousiastelingen.

Zonder de pretentie te hebben om ook maar enigszins compleet te zijn, zou je kunnen denken aan:

- **Een privacybeleid**
  Niet alleen grotere verenigingen hebben er veel baat bij als ze goed documenteren hoe ze met privacy omgaan. Dat is voor iedereen handig, omdat volgende besturen dan niet opnieuw het wiel hoeven uit te vinden. In dat beleid (of in een aantal procedures) kun je vastleggen hoe de diverse verantwoordelijkheden zijn geregeld en hoe je omgaat met foto's en ander beeldmateriaal van leden en niet-leden, om maar enkele voorbeelden te noemen.

- **Een privacyverklaring**
  Leden hebben er recht op om te weten hoe er met hun persoonsgegevens wordt omgegaan. Laat je dus inspireren door de duizenden *privacy statements* die op internet te vinden zijn en informeer ook jouw leden over jullie omgang met hun persoonlijke data. Je zou hen bijvoorbeeld bij aanmelding een mooie privacybrochure kunnen geven. Zie ook het antwoord op vraag 6. Welke privacy-informatie moeten we op de website zetten?

- **Een privacyportefeuillehouder**
  Neem "privacy" op in de portefeuille van een van de bestuursleden. Die persoon kan zich er dan extra in verdiepen en kan

optreden als vraagbaak, aanspreekpunt en contactpersoon. Zie ook het antwoord op vraag 10. Moeten de bestuurs- of commissieleden een soort privacyovereenkomst ondertekenen?

- **Een privacycommissie**
  Grotere verenigingen zouden kunnen overwegen een privacy-commissie in het leven te roepen. Die kan zich buigen over het formuleren van beleid en het werken aan de bewustwording van de leden. Vaak is er wel een energieke student Rechten te vinden die zo'n commissie wil leiden. Staat goed op je CV!

- **Een beveiligingstechneut**
  Niet iedereen weet even veel van informatiebeveiliging, maar het beveiligen van persoonsgegevens is een primaire taak van de vereniging. Probeer daarom iemand te vinden die verstand heeft van informatietechnologie en bombardeer die persoon (als-ie te vertrouwen is!) tot Head of Security of Voorzitter van de beveiligingscommissie.

- **Een verwerkingsregister**
  Voor de meeste verenigingen is zo'n register verplicht. Zie het antwoord op vraag 3. Moeten we een verwerkingsregister bijhouden?

- **Een datalekregister**
  In het datalekregister moet je bijhouden welke *inbreuken in verband met persoonsgegevens* er zijn opgetreden. Zie het antwoord op vraag 9. Wat moeten we doen bij een datalek?

2. In welke situaties moeten we om toestemming vragen?

Voor het verwerken van persoonsgegevens heb je soms toestemming nodig. Persoonsgegevens zijn bijvoorbeeld namen, contact- en studiegegevens, uitspraken en foto's. Met sommige persoonsgegevens van leden mag je bepaalde dingen doen omdat dat nu eenmaal nodig is om je vereniging goed te laten functioneren. Je hebt dan geen toestemming nodig, want als vereniging heb je goede redenen om die dingen te doen, en je leden verwachten ook dat je die dingen met hun persoonsgegevens doet. Die verwachting is heel belangrijk.

Dit klinkt misschien nogal vaag. Daarom vind je hieronder een tabelletje met enkele voorbeelden van dingen die je zonder toestemming mag doen en dingen waar je wél toestemming voor nodig hebt:

Géén toestemming nodig	**Wél toestemming nodig**
Namen van leden opnemen in interne publicaties (bijv. nieuwsbrieven en jaarboeken)	Contactgegevens van leden opnemen in interne publicaties (bijv. nieuws-brieven en jaarboeken)
Leden opnemen in de ledenadministratie	Informatie over niet-leden bijhouden
Persoonsgegevens van leden gebruiken om contributie te innen	Persoonsgegevens van externe personen gebruiken om ze te bestoken met spam
Nieuwsbrieven versturen aan leden (leden moeten zich wel kunnen uitschrijven)	Nieuwsbrieven versturen aan externe personen, incl. aspirant-leden (aanmelding geldt hier als toestemming)

Géén toestemming nodig	Wél toestemming nodig
Leden uitnodigen voor vergaderingen en evenementen	Externe personen uitnodigen voor vergaderingen en evenementen (aanmelding geldt hier als toestemming)
Een smoelenboek van leden samenstellen voor intern gebruik (leden moeten wel bezwaar kunnen maken)	Een smoelenboek extern beschikbaar stellen
Noodzakelijke persoons-gegevens verwerken van leden die zich hebben opgegeven voor een evenement (bijv. een reis)	Persoonsgegevens bewaren, zodat deze voor een volgend evenement niet opnieuw opgegeven hoeven te worden
Oud-leden die nog niet zo lang geleden actief zijn geweest, benaderen met nieuwsbrieven en/of uitnodigingen	Oud-leden die al vele jaren niet meer actief zijn geweest, ineens nieuwsbrieven gaan sturen

Voor **toestemming** gelden enkele belangrijke regels:

- Je moet kunnen aantonen dat iemand toestemming heeft gegeven. Mondelinge toestemming is meestal moeilijk aantoonbaar. Zorg dus voor een bewijs.
- Als iemand ergens toestemming voor heeft gegeven, moet die persoon die toestemming ook weer kunnen intrekken – zonder opgaaf van redenen.

Nog even over **nieuwsbrieven**: de ontvangers moeten altijd de mogelijkheid hebben om zich uit te schrijven. Dat uitschrijven mag niet nodeloos ingewikkeld zijn. Zorg er daarom voor dat er in elke nieuwsbrief een uitschrijfknop of -link aanwezig is.

Wat je met **foto's** mag doen, lees je in vraag 7. Wat mogen we doen met foto's waar mensen op staan?

3. Moeten we een verwerkingsregister bijhouden?

Een verwerkingsregister is een overzicht van alle “verwerkingen” met “persoonsgegevens” (zie vraag 2. In welke situaties moeten we om toestemming vragen?) die er binnen de vereniging plaatsvinden. Een “verwerking” kan werkelijk alles zijn wat je met persoonsgegevens kunt doen: van verzamelen, opslaan, inzien en kopiëren tot uitwisselen, archiveren en wissen. Dat laatste realiseren veel mensen zich niet.

De meeste organisaties zijn op grond van de AVG verplicht om een verwerkingsregister bij te houden. Er is echter een uitzondering gemaakt voor organisaties met minder dan 250 medewerkers. De kans is groot dat jouw vereniging inderdaad minder mensen in dienst heeft. Maar juich niet te vroeg, want er is ook nog een uitzondering op de uitzondering. Je moet als kleine organisatie namelijk wél een verwerkingsregister bijhouden als je “structureel” persoonsgegevens verwerkt. En bij een vereniging is dat nu eenmaal het geval. Denk bijvoorbeeld alleen al aan de ledenadministratie. Het antwoord op de vraag “moeten we een verwerkingsregister bijhouden” is dus JA. Doe je het niet, dan kan dit de vereniging een boete van de Autoriteit Persoonsgegevens opleveren.

Het lijkt heel wat, zo’n verwerkingsregister. Maar als studie- of studentenvereniging kun je je register gewoon opslaan in een Excel-bestand met minimaal de volgende kolommen voor elke verwerking:

Kolom in register	**Voorbeeld / *Opmerking***
Naam van de verwerking	Nieuwsbrieven verzenden
Doel van de verwerking	Het verzenden van nieuwsbrieven zodat de abonnees geïnformeerd blijven over

Kolom in register	Voorbeeld / *Opmerking*
	ontwikkelingen binnen (en buiten) onze vereniging
Verantwoordelijke voor de gegevens	Bestuurslid Externe contacten
Categorieën betrokkenen	Abonnees, zijnde: Leden van onze vereniging Oud-leden van onze vereniging Belangstellenden (na aanmelding)
Categorieën persoonsgegevens	Namen E-mailadressen
Bewaartermijn(en)	*Bedenk hoe lang het nodig is om gegevens te bewaren.* *Zie bijvoorbeeld ook vraag 4. Mogen we de persoonsgegevens van oud-leden bewaren en gebruiken?*
Ontvangers	***Let op:** Dit zijn dus niet de ontvangers van de nieuwsbrief, maar de eventuele ontvangers van persoonsgegevens. Soms zou dit bijvoorbeeld de Universiteit Utrecht kunnen zijn.*
Toegankelijk voor	Bestuurslid Externe contacten Leden Nieuwsbriefcommissie
Gebruikte software	Excel (adressenbestand) Maileon (verzendsoftware)
Beveiliging	Wachtwoord (bestand in Excel)
Export buiten de EER?	Nee *Vul hier Ja in als je binnen deze verwerking persoonsgegevens verstuurt naar een land buiten de EER (d.w.z. de EU plus IJsland, Noorwegen en Liechtenstein)*

Tip! Waarom zou je het wiel opnieuw uitvinden? Kijk eens bij een zustervereniging hoe hun verwerkingsregister er uitziet. Vaak komen de registers van vergelijkbare verenigingen voor een groot deel overeen.

4. Mogen we de persoonsgegevens van oud-leden bewaren en gebruiken?

Het antwoord op deze vraag is best ingewikkeld, want het is afhankelijk van verschillende factoren. Al die factoren hebben op de een of andere manier te maken met de verwachtingen van die oud-leden, namelijk:

Mogen de oud-leden redelijkerwijs verwachten dat je nog persoonsgegevens van hen bewaart?

Stel jezelf de volgende vragen:

- **Zijn de oud-leden nog (enigszins) actief binnen de vereniging?**
  Oud-leden die nog af en toe actief zijn, verwachten dat je persoonsgegevens van hen bewaart. Ze willen immers in contact blijven.
- **Zo nee: hoe lang zijn ze al niet meer actief?**
  Oud-leden die niet meer actief zijn, kunnen soms wel weer actief worden, bijvoorbeeld naar aanleiding van een lustrumviering. Voor het vieren van een lustrum mag je – in principe – contactgegevens bewaren. Zo'n lustrum is dan ook meteen een goede gelegenheid om te controleren of de gegevens nog kloppen. Je bent namelijk verplicht om ervoor te zorgen dat de persoonsgegevens die je bewaart *correct* zijn.
- **Welke gegevens zou je willen bewaren?**
  Namen zijn de meest elementaire gegevens die je zou willen bewaren. In het kader van de geschiedschrijving van je vereniging valt er iets voor te zeggen om die gegevens alleen op verzoek te vernietigen. Bij contactgegevens ligt dat anders. Die verouderen snel. Het ligt niet voor de hand dat een lid na dertig jaar nog op dezelfde studentenkamer woont. Maar wanneer oud-leden bereid zijn hun adreswijziging met je te delen, geven

ze impliciet toestemming om die gegevens ook gedurende een redelijke termijn te bewaren en te gebruiken.

- **Hadden de oud-leden indertijd een specifieke functie binnen de vereniging?**
  De samenstelling van besturen en commissies is van belang in het kader van de geschiedschrijving van je vereniging. Geef jaar- of lustrumboeken uit, dan is die samenstelling daar vaak in te vinden. In dat geval is het dus niet nodig om voor dat doel nog extra informatie te bewaren.

5. Mogen we gegevens opslaan in de cloud?

De cloud is vaak een heel gemakkelijke – en veilige! – manier om gegevens op te slaan en uit te wisselen. Voor verenigingen is het opslaan van gegevens in de cloud toegestaan, zij het onder bepaalde voorwaarden.

Studieverenigingen binnen de UU kunnen gebruikmaken van Microsoft Onedrive. De UU heeft een zogenoemde verwerkers-overeenkomst met Microsoft gesloten. Daarin is vastgelegd wat Microsoft wél met de gegevens mag doen (niet veel), en wat níet (bijvoorbeeld exporteren naar een land buiten de EU). Bij gebruik van Microsoft Onedrive zit je dus meestal goed.

Diensten als Google Drive en Dropbox exporteren de gegevens vaak wél naar landen buiten de EU (bijvoorbeeld naar de VS). Met die bedrijven heeft de UU trouwens ook geen verwerkers-overeenkomst gesloten. Het gebruik van deze diensten wordt daarom ontraden. Het zal allemaal zo'n vaart niet lopen, maar zeker als het gaat om zeer vertrouwelijke persoonsgegevens (zoals parpoortnummers die nodig zijn voor een reis), neem je met deze cloud providers een onnodig risico.

6. Welke privacy-informatie moeten we op de website zetten?

Welke privacy-informatie je op de website moet zetten, hangt ervan af waar je de website voor gebruikt en hoe je dat doet.

- **Gebruik je de website alleen om informatie over je vereniging te verstrekken** (zonder informatie binnen te halen)? Dan is het niet verplicht om privacy-informatie op de website te plaatsen. Maar de website is natuurlijk een ideale plek om leden via een privacyverklaring te laten weten hoe je met hun persoons-gegevens omgaat. Desnoods zet je die informatie in een gedeelte van de website dat alleen toegankelijk is voor leden.
- **Gebruik je de website ook om informatie te verzamelen**, bijvoorbeeld door de mogelijkheid te bieden om informatie aan te vragen? Dan moet je op de pagina waarop iemand zijn of haar gegevens invult, laten weten (bijvoorbeeld via een link) wat je met die persoonsgegevens gaat doen: Voor welk doel gebruik je ze? Hoe lang ga je ze bewaren? Hoe zijn ze beveiligd? Welke rechten heeft de invuller met betrekking tot die gegevens? En zo zijn er nog een paar vragen. Voorbeelden van zulke privacyverklaringen zijn overal op internet te vinden.
- **Wil je cookies plaatsen**? Dan moet je voor het plaatsen van niet-noodzakelijke cookies toestemming vragen aan de gebruiker. (Noodzakelijke cookies mag je ook zonder toestemming plaatsen.) Die toestemming moet “geïnformeerd” zijn. Dat wil zeggen dat je alle informatie moet verstrekken die voor de gebruiker van belang kan zijn bij de beslissing om toestemming te verlenen of niet.

  Let op! Bij het vragen om toestemming mag het vakje waarmee de gebruiker toestemming kan geven, niet vooraf aangevinkt zijn. Dan is de toestemming namelijk niet geldig.

7. Wat mogen we doen met foto's waar mensen op staan?

N.B. Het onderstaande geldt voor foto's én video's!

Heb je foto's waar mensen op staan en wil je die alleen **intern verspreiden**? Dan mag dat als aan al de volgende voorwaarden is voldaan:

1. de gefotografeerde personen hebben geen bezwaar gemaakt tegen interne publicatie;
2. de foto's zijn niet compromitterend of op een andere manier onprettig (en ze kunnen redelijkerwijs ook niet zo worden ervaren);
3. je hebt in je privacybeleid en je privacyverklaring voor leden vastgelegd dat er op deze manier met foto's wordt omgegaan.

Als je weet of kunt vermoeden dat iemand niet blij is met de verspreiding van een foto waar hij of zij op staat, dan mag je die foto echt niet verspreiden, ook niet intern. Toestemming vragen is dan het devies. En heb je de foto al geplaatst, dan moet je hem verwijderen als de onfortuinlijke gefotografeerde bezwaar aantekent.

Voor het **extern verspreiden** van foto's waar mensen herkenbaar op te zien zijn, heb je in beginsel de toestemming van diegenen nodig, of je moet die personen *blurren*. Op internet zijn standaard toestemmingsformulieren te vinden. Het gaat daarbij om zogenoemde *quitclaims*. Op die formulieren kun je aangeven waar de foto voor mag worden gebruikt, waar hij mag worden geplaatst, voor hoe lang, of ook de naam van de gefotografeerde mag/moet worden vermeld, of de foto bewerkt mag worden, of de foto pas mag worden geplaatst nadat de gefotografeerde het eindresultaat heeft gecontroleerd, of het om een specifieke foto of om alle foto's

gaat, noem maar op. Het belangrijkste is dat je duidelijke en aantoonbare afspraken maakt.

Let op! Wist je dat het niet toegestaan is om in de collegezalen van de Universiteit Utrecht foto- of video-opnamen te maken? Wil je dat wél doen, dan moet je de docent om uitdrukkelijke toestemming vragen. De opnamen die je dan maakt, zijn uitsluitend voor eigen gebruik; je mag ze hoe dan ook niet op sociale media plaatsen, ook niet met toestemming van de docent.

8. Wanneer hebben we een verwerkersovereenkomst nodig?

Een verwerkersovereenkomst is een document waarin een opdrachtgever (de *verwerkingsverantwoordelijke*) en een opdrachtnemer (de *verwerker*) vastleggen wat hun rechten en (vooral) plichten zijn bij het verwerken van persoonsgegevens.

Huurt jouw vereniging een bedrijf of particulier in om in jullie opdracht iets met persoonsgegevens te doen (bijvoorbeeld cloudopslag, administratieve taken etc.), dan moet jouw vereniging afspraken maken met dat bedrijf of die particulier. Maar let op: dat hoeft alléén als die opdracht specifiek bedoeld is om iets met persoonsgegevens te doen (bijvoorbeeld data-analyse). Geef je bijvoorbeeld een pakketdienst opdracht om een pakketje te bezorgen, dan zijn er voor die bezorging wel persoonsgegevens nodig (naam en adres), maar de verwerking van die persoonsgegevens is niet het hoofddoel. Met andere woorden: je hoeft geen verwerkersovereenkomst af te sluiten.

Het zal dus niet zo vaak voorkomen dat je een verwerkers-overeenkomst moet afsluiten. En moet dat wél, dan heeft de opdrachtnemer meestal wel een standaardmodelletje op de plank liggen.

9. Wat moeten we doen bij een datalek?

Het eerste wat je moet doen, is het datalek *herkennen*! De meeste mensen denken bij een datalek aan een gestolen of vergeten laptop of USB-stick, een verkeerd geadresseerde mail of een hacker die met satanisch genoegen hun meest waardevolle data steelt of vergrendelt.

Dat zijn inderdaad allemaal voorbeelden van datalekken. Maar het begrip datalek is veel breder, want wat in de volksmond gewoon een datalek heet, staat in de wet bekend als *een inbreuk in verband met persoonsgegevens*. En daar vallen ook situaties onder waarbij gegevens bijvoorbeeld niet meer toegankelijk zijn (of gewist) en waarbij gegevens per ongeluk of opzettelijk zodanig zijn gewijzigd dat ze niet meer kloppen.

Op de website van de Autoriteit Persoonsgegevens (AP) vind je een handig overzicht van de stappen die je moet zetten als (je vermoedt dat) er een datalek is opgetreden. Zie https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stappenplan_actie_datalek.pdf

In het kort:

1. Zorg dat je een goed beeld krijgt van de situatie.
2. Neem maatregelen om de schade te beperken.
3. Meld het lek *binnen 72 uur* bij de AP (indien nodig).
4. Licht de slachtoffers in (indien nodig).
5. Registreer het lek in je datalekregister (zie vraag 1. Wat moeten we als vereniging allemaal regelen?).

10. Moeten de bestuurs- of commissieleden een soort privacyovereenkomst ondertekenen?

Nee, het is niet nodig om in een overeenkomst vast te leggen dat je de privacywetgeving zult naleven. Van bestuursleden wordt – net als van commissieleden – verwacht dat ze zich aan de wet houden; dat hoeven ze niet ook nog eens in een extra verklaring of overeenkomst te bevestigen.

Wel is het verstandig om binnen het bestuur een portefeuille-houder Privacy aan te wijzen. Dat is degene die zich nét iets meer dan de anderen in privacyzaken verdiept en die ook kan fungeren als aanspreekpunt voor leden en externe partijen.

Universiteit Utrecht

Meer informatie

Studieverenigingen hebben meestal een band met een bepaalde studierichting of faculteit. Formeel zijn het echter afzonderlijke rechtspersonen die hun eigen boontjes moeten doppen. Maar we willen jullie niet helemaal in de kou laten staan. Voor (een beperkte hoeveelheid) extra informatie kun je terecht bij de privacy officer van de faculteit waar je affiniteit mee hebt. De mailadressen vind je op het UU intranet.

Studentenverenigingen hebben weliswaar een duidelijke binding met de universiteit, maar ze kunnen niet worden gezien als onderdeel ervan. Zij zullen voor extra ondersteuning moeten aankloppen bij externe partijen.

Handige links:

- Alle studenten die verbonden zijn aan de UU kunnen uiteraard de intranetpagina's over privacy lezen. intranet.uu.nl/privacy
- Website van de Autoriteit Persoonsgegevens: www.autoriteitpersoonsgegevens.nl
- Tekst van de AVG in alle talen van de EU: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex%3A32016R0679
- Document *Studieverenigingen bij de UvA en de AVG*[1] https://beeldbank.uva.nl/m/71be992001816a73/original/studieverenigingen-bij-de-uva-en-de-avg-1-2-opgemaakt.pdf
- Het *Studentenstatuut* van de UU: https://students.uu.nl/praktische-zaken/regelingen-en-procedures/oer-en-studentenstatuut#Studentenstatuut

[1] Dit document van de Universiteit van Amsterdam was de inspiratiebron voor De AVG in 10 vragen *(en antwoorden)*