# Privacybeleid studentenpartij **asap**

## 1. Inleiding

### 1.1 Vereisten verwerking persoonsgegevens voor verenigingen

De Wet bescherming persoonsgegevens stelt eisen aan organisaties die gegevensbestanden beheren, zoals een ledenadministratie. Deze eisen zijn als volgt:

- Een lid moet toestemming geven voor het verwerken zijn/haar gegevens;
- De gegevens van het lid moet op een juiste en nauwkeurige manier bijgehouden worden;
- De gegevens van het lid moet beveiligd worden;
- Op verzoek inzage verlenen in de eigen opgeslagen gegevens van het lid;
- Het uitsluitend gebruiken van de gegevens van het lid voor het doel waarvoor ze verzameld zijn.

Conform de Wet bescherming persoonsgegevens is het studentenpartij **asap** toegestaan persoonsgegevens te verwerken; categorie Bijzondere vereisten, vrijgestelde categorieën van verwerkingen (paragraaf 1): verenigingen, stichtingen en publiekrechtelijke beroepsorganisaties.

### 1.2 Systemen

Studentenpartij **asap** maakt gebruik van de volgende systemen voor het verwerken van persoonsgegevens:

#### 1.2.1 Conscribo

Conscribo is de administratieve applicatie van studentenpartij **asap**. In dit programma verwerken wij de lidmaatschapsgegevens en dit programma wordt ook gebruikt voor de financiële administratie.

#### 1.2.2 Mailchimp

Mailchimp is de geautomatiseerde applicatie waarin studentenpartij **asap** haar nieuwsbrieven maakt. Tevens verstuurt Mailchimp de nieuwbrieven maandelijks.

#### 1.2.3 One.com

One.com wordt gebruikt voor alle inkomende en uitgaande mails van **asap**. Ieder bestuurslid heeft een eigen account via welke hij of zij e-mails kan sturen naar leden.

### 1.3 Privacy statement

Studentenpartij **asap** verwerkt persoonsgegevens en wil daarover duidelijk en transparant communiceren. In het privacy statement wordt antwoord gegeven op de belangrijkste vragen over de verwerking van persoonsgegevens door studentenpartij **asap**. Het privacystatement is te vinden op de website en is als bijlage toegevoegd bij dit document

### 1.4 Updates privacybeleid

Studentenpartij **asap** behoudt zich het recht om wijzigingen aan te brengen in dit privacybeleid. Het verdient aanbeveling om dit privacybeleid regelmatig te raadplegen, zodat je van de wijzigingen op de hoogte bent. Je kunt dit privacybeleid zelf opslaan of raadplegen via de website.

## 2. Informatie

### 2.1 Dataverzameling en zichtbaarheid

De volgende categorieën persoonsgegevens onderscheiden wij

- Data identiteit: naam, geboortedatum, lidmaatschapsnummer, studentnummer

- Data contact: fysiek adres (postcode, straatnaam, huisnummer), mail, telefoonnummer
- Data financieel: banknummer, volledige naam, datum inschrijving en uitschrijving

| | Verplicht voor lidmaatschap | Optioneel | Zichtbaar voor penningmeester | Zichtbaar voor secretaris | Zichtbaar voor lid |
|---|---|---|---|---|---|
| Voornaam | X | | X | X | |
| Voorletters | X | | X | X | |
| Achternaam | X | | X | X | |
| Adres/postcode/woonplaats | | X | X | X | |
| Telefoonnummer | | X | X | X | |
| Geslacht | | X | X | X | |
| Geboortedatum | X | | X | X | |
| Studentnummer | | X | X | X | |
| Bankrekening | X | | X | | |
| Datum inschrijving/uitschrijving | X | | X | X | |
| Mailadres | X | | X | X | |
| Lidmaatschapsnummer | X | | X | X | |
| Machtigingen | X | | X | | |

**2.2 Systeem en gegevensbeheer**

Studentenpartij **asap** beschikt momenteel niet over een eigen hardware. Om deze reden wordt alle informatie opgeslagen in een cloud. Alleen het bestuur beschikt over de inlogcodes van deze clouddienst en zal deze ook nooit ter beschikking stellen voor derden. Het spreekt voor zich dat de afzonderlijke hardware die de bestuursleden privé gebruiken om gegevens in te zien, beschikken over de nodige specificaties om data veilig te kunnen verwerken.

**2.3 Permissies**

De penningmeester en secretaris van **asap** dragen de verantwoordelijkheid voor de gegevensverwerking. Alleen zij zijn gemachtigd binnen het bestuur om persoonsgegevens te verwerken.

**3. Verstrekken uitwisselen en gebruik van persoonsgegevens**

**3.1 Algemeen**

3.1.1 Wie verwerkt

- Personen zelf
- Penningmeester
- Secretaris

3.1.2 Voorwaarden gebruik persoonsgegevens

Het gebruik van gegevens dient aan de volgende voorwaarden te voldoen:

1. Er moet een duidelijk doel zijn gesteld waartoe de gegevens gebruikt worden, waarbij duidelijk wordt wie voor welke periode toegang heeft tot welke gegevens;
2. Er mogen enkel relevante gegevens gebruikt worden. Met andere woorden, er mogen geen onnodige of bovenmatige gegevens verzameld of gebruikt worden;
3. Er dient een permissiemodel opgesteld te worden waarin wordt vastgelegd welke personen toegang krijgen tot welke gegevens. Tevens dient er een gedegen beveiliging te worden aangebracht op het gebruik van de gegevens;
4. De gegevens mogen niet aan derden worden verstrekt tenzij daar expliciet toestemming voor gegeven is door het lid of daartoe een wettelijke verplichting bestaat;

5. De gegevens mogen alleen voor een vastgestelde periode worden gebruikt en dienen daarna verwijderd te worden. Tussentijds moeten gegevens op het verzoek van het lid verwijderd kunnen worden. Langer gebruik dan de vooraf vastgestelde periode (bijvoorbeeld voor de duur van een evenement) kan alleen met expliciete toestemming van het lid;
6. Bijzondere gegevens, waaronder godsdienst, gezondheid of strafrechtelijke gegevens, mogen alleen verzameld worden indien daartoe een strikte noodzaak bestaat en met expliciete consensus van het lid. Deze gegevens dienen volledig te worden verwijderd na afloop van de gestelde periode;
7. Het gebruik van de gegevens gebeurt conform het privacybeleid en de Wet bescherming persoonsgegevens.

3.1.3 inschrijving voor een activiteit
Voor een activiteit kunnen en mogen er lidmaatschapsgegevens gebruikt worden, mits hier toestemming voor is gegeven en aan de volgende voorwaarde is voldaan:

- Er staat beschreven dat de gegevens uitsluitend voor dit evenement gebruikt zullen worden;
- Er is een OPT-in voor het gebruik van contactgegevens (bijvoorbeeld: adres, telefoonnummer en e-mail). Een OPT-out mogelijkheid is verplicht;
- De gegevens mogen alleen gebruikt worden voor het evenement waarvoor iemand is aangemeld. Het is niet toegestaan de gegevens te gebruiken voor promotie van de activiteit van het daaropvolgende jaar, behalve als hiervoor is gekozen met een aparte OPT-in optie.

**4. Mutaties in persoonsgegevens**
**4.1 Wie kan muteren**

- Het lid zelf
- De gegevensbeheerder

4.1.1 Mutatie door leden
Een lid kan te allen tijde de opgeslagen gegevens opvragen bij het bestuur. Deze zullen binnen de termijn van één maand worden verstrekt. Hierop kan desbetreffende lid mutaties voorstellen, m.u.v. het lidmaatschapsnummer.

4.1.2 Mutaties door gegevensbeheerder
De gegevensbeheerder kan alle persoonsgegevens van een lid muteren.

**5. Bewaren van persoonsgegevens**
De gegevens die opgeslagen zijn in Conscribo blijven hierin verwerkt zolang het lidmaatschap van het lid loopt. Dit omvat zowel de persoons- als de bankgegevens. Na afloop van het lidmaatschap worden de gegevens bewaard tot het einde van het academisch jaar, waarna ze gearchiveerd zullen worden. De gegevens van oud-leden kunnen niet gewijzigd worden en dienen uitsluitend voor historische doeleinden, alsmede het organiseren van een reünie en het kunnen uitvoeren van een alumnibeleid. Deze zijn alleen inzichtelijk voor het bestuur.

**6. Berichtgeving**
Alle berichtgeving van studentenpartij **asap** geschiedt ofwel via de mail van onze webhosting, dan wel via Mailchimp voor de nieuwsbrieven.

Voor de nieuwsbrief is er een OPT-out optie waarin leden zich kunnen uitschrijven. Uitschrijven is mogelijk door een mail te sturen naar de secretaris. Deze optie wordt actief aangeboden.

De mailing vanuit de webhosting, m.a.w. mails direct afkomstig van het bestuur, hebben geen OPT-out mogelijkheid, omdat deze mails noodzakelijk zijn voor het functioneren als lid binnen de vereniging. Hierbij kan gedacht worden aan uitnodigingen voor een Algemene Ledenvergadering.

**8. Datalekken**

Uiteraard doet studentenpartij **asap** er alles aan om de, in dit document genoemde, persoonsgegevens niet in handen van derden te laten vallen. Gebeurt dit wel, dan spreken we over een datalek. In artikel 34a van de Wet Bescherming Persoonsgegevens staat sinds 1 januari 2016 vermeld dat een datalek gemeld moet worden. Er wordt hier echter met klemtoon gesproken over het lekken van persoonsgegevens als gevolg van beveiligingsproblemen. Deze datalekken moeten, wanneer voldoende ernstig van aard, onverwijld worden gemeld aan de toezichthouder: de Autoriteit Persoonsgegevens (AP), voorheen het CBP.

8.2 Procedure datalekken communiceren

*8.2.1* Aan de toezichthouder

Zodra er sprake is van een datalek zal dit binnen 72 uur gemeld moeten worden bij de toezichthouder, zoals hiervoor genoemd. De melding hiervan bevat tenminste:

- De aard van de inbreuk;
- De instantie(s) waar meer informatie over de inbreuk kan worden verkregen;
- De aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken;
- Een beschrijving van de geconstateerde en vermoedelijke gevolgen van de inbreuk voor de verwerking van de persoonsgegevens;
- De maatregelen die de organisatie heeft genomen of voorstelt te nemen om deze gevolgen te verhelpen.

8.2.2 Aan het lid

Nadat er een datalek heeft plaatsgevonden en het waarschijnlijk is dat het lek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van het betrokken lid, dient dit lid een melding te ontvangen. In deze melding zal tenminste de aard van de inbreuk, de instantie(s) waar meer informatie over de inbreuk kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken bevatten.

**9. Misbruik van persoonlijke gegevens**

9.1 Misbruik voorkomen

Wanneer persoonsgegevens gebruikt worden op een andere manier dan is toegestaan volgens wet en beleid, dan is er sprake van ongeoorloofd gebruik. Het ongeoorloofd gebruik kan onopzettelijk zijn, omdat men niet op de hoogte is van de regels. Er kan ook sprake zijn van opzet. In het kader van dit beleid verstaan we onder het begrip ‘misbruik’ zowel opzettelijk als onopzettelijk ongeoorloofd gebruik. Misbruik kan leiden tot schade aan personen of de organisatie.

We spreken over misbruik, wanneer:

- Een persoon die daartoe niet gerechtigd is gegevens verkrijgt en gaat gebruiken.
- Een, in principe gerechtigd, persoon de gegevens gebruikt voor een ander doel dan dat (hem) is toegestaan.
- Gegevens gebruikt worden die niet geregistreerd of gebruikt mogen worden.

Om misbruik te voorkomen is het belangrijk dat een aantal maatregelen getroffen worden. Zo is het belangrijk om beleid op het gebied van privacy en persoonsgegevens te hebben, afspraken te maken en deze duidelijk te communiceren. Duidelijkheid over goed gebruik van gegevens voorkomt in ieder geval onopzettelijk misbruik.

9.1.2 Integriteits- en geheimhoudingsverklaringen
Personen die breed toegang hebben tot gegevens moeten bij aanvang van hun taak of functie een integriteits- en geheimhoudingsverklaring ondertekenen. In die verklaring staat beschreven dat er zorgvuldig moet worden omgegaan met gegevens, waaronder persoonsgegevens.

9.2 Misbruik melden
Wanneer iemand een vermoeden heeft dat er misbruik wordt gemaakt van persoonsgegevens binnen de partij, dient dit gemeld te worden bij het bestuur van deze, zodat er waar nodig maatregelen getroffen kunnen worden. Zie voor contactgegevens en procedure hoofdstuk 10.

9.3 Maatregelen
Misbruik van gegevens zal – afhankelijk van de ernst - aanleiding geven tot een van de volgende maatregelen: waarschuwing, ontzeggen toegang tot gegevens, beëindigen functie of taak en eventueel einde lidmaatschap. Er zal daarnaast ook steeds worden onderzocht of dit misbruik voorkomen kan worden.

10 Vragen en klachten
Vragen kunnen gesteld worden door een mailtje te sturen naar secretaris@asapnijmegen.nl.

Ook voor een klacht of melding kun je hier terecht.
Van elke melding zullen de nodige gegevens worden geregistreerd. Hierdoor kan, tijdens behandeling, het nodige contact onderhouden worden met degene die contact met **asap** op heeft genomen.

Bij elke melding zal achterhaald worden:

- Waar de gebruikte gegevens vandaan komen;
- Wat er met de gegevens is gebeurd;
- Wie er betrokken is;
- Of er schade is ontstaan en hoe die zoveel mogelijk te herstellen is;
- Welke stappen nodig zijn om herhaling te voorkomen.