Informatiebrochure AVG (Algemene Verordening Gegevensbescherming) voor verenigingen etc. aangesloten bij KLN en NBS

Inhoudsopgave

Vooraf

De AVG is een aanvulling op de Wet Bescherming Persoonsgegevens waarin al veel van de in de AVG opgenomen verplichtingen waren opgenomen. Alleen dat was in het verleden nooit goed gecommuniceerd met bedrijven etc. waardoor iedereen nu op het laatst allerlei zaken moet regelen voor de AVG.
De AVG gaat over het (digitaal) registreren van persoonsgegevens (zoals naam, adres, postcode, woonplaats, telefoonnummers, banknummers, specifieke ledeninformatie etc.) en **vooral** hoe e.e.a. is beveiligd. Niet alleen digitaal maar bijvoorbeeld ook als de gegevens "gestructureerd" op papier staan.
U leest regelmatig berichten in de media over datalekken; laatst nog van Facebook. Daar gaat de AVG juist over.

Het is heel belangrijk dat u als relatief kleine organisatie uw goede wil toont! Het hoeft niet perfect te zijn, als u maar kunt aantonen dat u uw best heeft gedaan. Niets doen is geen optie omdat de AP (Autoriteit Persoonsgegevens) op iedere klacht moet reageren en stevige boetes kan opleggen. Nu zal dat bij een kleine vereniging meevallen maar toch … Nationale tentoonstellingen hebben soms duizenden personen in hun bestanden staan. Dan wordt een datalek toch serieus.

Daarnaast is in de AVG iets wezenlijks gewijzigd namelijk een organisatie moet nu aantonen dat op een juiste manier met de gegevens en beveiliging wordt omgegaan (verantwoordingsplicht!).

Het is uw verantwoordelijkheid om de vereisten uit de AVG te regelen. Middels deze informatiebrochure willen wij u een handreiking geven. Als u daarna nog vragen heeft, kunt u daarmee altijd terecht bij de toezichthoudende instantie: de Autoriteit Persoonsgegevens (AP).

Attentiepunten

Belangrijkste attentiepunten voor u zijn:

- Inventariseer welke gegevensregistraties uw vereniging heeft en waar deze staan.
- Heeft u een website met bijv. contactformulieren, formulieren om nieuwe leden door te geven e.d. dan moet u de website beveiligen en op de betreffende pagina's een link naar uw privacyverklaring opnemen.
- U moet registers aanleggen voor registratie van:
    - uw persoonsgegevensregistraties die u verwerkt;
    - datalekken;
    - persoonsgegevens die u als bewerker van een andere organisatie onder u hebt.
- Controleren of u catalogi met inzenderslijsten op de website heeft staan (inzenderslijst verwijderen).
- Controleer of u ledenlijsten op de website heeft staan die niet in een besloten deel achter een toegangscode en wachtwoord staan (complete ledenlijst van de website halen).
- Staat er info van leden/fokker/anderen met persoonsgegevens en bijv. de rassen en kleuren die zij fokken: direct expliciet aan hen toestemming vragen anders van de website verwijderen.
- Nooit mailingen versturen met alle mailadressen zichtbaar in het veld Aan of het veld CC.
- Probeer voor ingangsdatum van de AVG (25 mei 2018) al wat te hebben vastgelegd, uw website op te schonen en aan te vullen.

Persoonsgegevens

Wat zijn persoonsgegevens

Alle digitale gegevens die betrekking hebben op, of te herleiden zijn naar een natuurlijk persoon (direct en indirect) vallen onder de noemer persoonsgegevens en die via een computer, tablet, smartphone etc. worden verwerkt. Ook als het gestructureerd op papier staat, zijn het persoonsgegevens die onder de AVG vallen.

Met de persoonsgegevens, die u verwerkt, moet u als een 'goed huisvader' omgaan. Ze moeten bijvoorbeeld beschermd zijn tegen verlies of inbreuk, niet langer worden bewaard dan noodzakelijk en u moet niet méér gegevens verzamelen dan nodig is om uw doel te bereiken.

Uw privé-lijstjes van familie e.d. vallen niet onder de AVG.

Registraties van persoonsgegevens

Belangrijk is om te inventariseren welke gegevensregistraties u als vereniging heeft. Iedere vereniging, ook al beseft u het niet, heeft meerdere gegevensregistraties zoals:

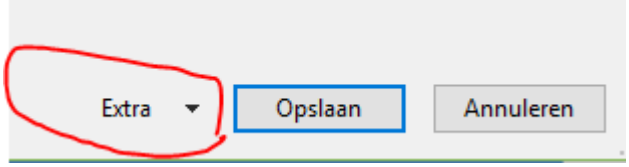
- De ledenadministratie zelf
- Lijst voor de tatoeëerder met gegevens van de konijnenfokkers
- Lijsten in tentoonstellingssoftware (inzenders, keurmeesters en medewerkers)
- Aparte lijsten voor versturen van vraagprogramma's
- Andere lijsten

Maar ook bij wie staan deze, bij wie staan (schaduw)kopieën en hoe is de computer beveiligd waarop deze gegevens staan?

Daarnaast zijn er nog meer registraties van persoonsgegevens waar u in 1^{e} instantie niet aan denkt zoals de debiteuren- en crediteurenadministratie in de boekhouding. Ook dit zijn persoonsgegevens. Denk ook aan oude registraties die u niet meer gebruikt maar nog wel heeft. Overweeg om deze te verwijderen, dan hoeft u ze ook niet te registreren. Denk wel aan de (fiscale) bewaarplicht wanneer u bijvoorbeeld belastingplichtig bent voor de omzetbelasting.

Al deze registratie van persoonsgegevens moet in een "register verwerkingen" worden vastgelegd met onder andere info van beveiliging (het bestand zelf) en de computer (virusscanner, inloggen op de pc met een wachtwoord etc.).

Tip:
Zet op alle bestanden die persoonsgegevens een (goed) wachtwoord zodat, wanneer uw computer wordt gehackt of zonder uw toestemming wordt gebruikt of wordt gestolen, deze niet makkelijk te raadplegen zijn door onbevoegden. Of gebruik encryptie.
Bij Excel bestanden kunt u een wachtwoord bij opslaan als en dan Extra aan te klikken.



Wanneer mag u persoonsgegevens registeren?

Voor het registreren van persoonsgegevens is wettelijke grondslag vereist. Zonder een grondslag mag u geen persoonsgegevens verwerken.
In de wet worden genoemd:

1. Toestemming
2. Uitvoering overeenkomst
3. Wettelijke verplichting
4. Vitaal belang
5. Publiekrechtelijke taak of algemeen belang
6. Gerechtvaardigd belang

De eerste twee zijn duidelijk; 3, 4 en 5 zullen bij kleindierverenigingen niet snel voorkomen. De 6e gerechtvaardigd belang behoeft toelichting.

Van een gerechtvaardigd belang kan sprake zijn wanneer er een 'relevante en passende verhouding' is tussen een organisatie en de persoon wiens gegevens door deze organisatie worden verwerkt. Deze grondslag is vaak van toepassing op direct marketing.
Zo'n verwerking mag alleen als de fundamentele rechten en vrijheden van de betrokkene niet zwaarder wegen. Denk hierbij bijvoorbeeld aan het recht op privacy van consumenten.

De grondslag voor verwerking van gegevens van leden (lidmaatschap) en inzenders van tentoonstelling ed. is een overeenkomst.

Bij uw verwerking van persoonsgegevens spelen nog een aantal beginselen een rol::

- Rechtmatigheid, behoorlijkheid en transparantie
- Doelbinding
- Minimale gegevensverwerking (niet meer dan strikt noodzakelijk voor het doel wat u wilt bereiken)
- Juistheid
- Opslagbeperking
- Integriteit en vertrouwelijkheid

U mag als kleindierorganisatie geen bijzondere persoonsgegevens registreren. Bijzondere persoonsgegevens zijn o.a. ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakvereniging, gezondheid en seksueel gedrag of seksuele gerichtheid. U hebt daarvoor namelijk geen wettelijke grondslag.

Overige begrippen voor de AVG

- Betrokkene: de mensen van wie de persoonsgegevens worden verwerkt.
- (Verwerkings)verantwoordelijke: bepaalt welke verwerking plaatsvindt van welke persoonsgegevens, voor welk doel en op welke wijze.
- Verwerker: verwerkt persoonsgegevens ten behoeve van de verantwoordelijke, zonder dat hij aan het rechtstreekse gezag van de verantwoordelijke is onderworpen.

Website

Website en invulformulieren

Inventariseer of uw website pagina's heeft om online gegevens in te vullen door nieuwe leden, om contact op te nemen e.d.

Is dat het geval, dan worden persoonsgegevens via uw website verwerkt en MOET het worden beveiligd. I.p.v. dat er boven in de adresbalk http:// etc. verschijnt moet daar komen https:// etc. (met een s).
Vraag uw website beheerder/organisatie bij wie u de website heeft staan een zogenaamd ssl-certificaat (beveiligingscertificaat – kwaliteit van de beveiliging is niet van belang) te installeren.

Een alternatief is om deze invulformulieren op uw website te verwijderen en alleen een link naar het e-mailadres van de secretaris op te nemen.

Privacyverklaring op de website

Wanneer u invulformulieren op de website heeft of een webshop, bent u verplicht een link naar de privacyverklaring op die pagina neer te zetten.

In de bijlagen is een checklist opgenomen. Met deze verklaringengenerator kunt u zelf een eenvoudige privacyverklaring maken die u nog kunt aanpassen:
https://veiliginternetten.nl/privacyverklaring-generator/start/

Website en gegevens van (niet-) leden

Controleer of op uw website contactgegevens van uw leden staan met bijvoorbeeld welke rassen en kleuren zij fokken. Zo ja, dan moeten zij u daarvoor uitdrukkelijk toestemming geven en deze toestemming moet u goed bewaren.
Voor bestaande vermeldingen moet u dus de betreffende leden aanschrijven om voor een bepaalde datum toestemming te geven. Krijgt u geen toestemming of geen antwoord dan moet u de gegevens van dat lid direct verwijderen.

Ledenlijsten mogen alleen op de website staan als zij in een alleen voor leden toegankelijke (besloten) deel achter een toegangscode en wachtwoord staan.
Of u moet een lijst op uw website opnemen van alleen leden die expliciet schriftelijk of per mail daarvoor toestemming hebben gegeven.
In Excel is het eenvoudig een kolom "Toestemming publicatie op website" toe te voegen en die met Nee te vullen. Krijgt u toestemming dan pas vult u Ja in. Bij het vragen van die toestemming moet u duidelijke uitleg geven waarvoor u die toestemming wilt gebruiken.

Website en cookies

Veel websites, ook verenigingswebsites, en social media kanalen werken met cookies. Het is verplicht om bezoekers hier op te wijzen.
Vraag bij u beheerder na of uw website cookies heeft of iets van Google Analytics waarbij gegevens over de bezoeker worden vastgelegd. Als het niet mogelijk is om dit uit te schakelen moet u dit in de privacyverklaring opnemen.

Mailings

Veel verenigingen sturen e-mails naar groepen leden of geïnteresseerden. Maar ook het verzenden van elektronische mailingen is aan regels gebonden.

Waar moet je op letten bij het versturen van mailingen per e-mail?

Het sturen van elektronische commerciële berichten (bijvoorbeeld via e-mail of persoonlijk bericht via social media) is een vorm van direct marketing. Daarvoor gelden bijzondere regels, ook wel de "SPAM-regels" genoemd. De SPAM-regels gelden voor het versturen van "ongevraagde" berichten, zoals nieuwsbrieven en reclame. Voor het versturen van zulke berichten heb je uitdrukkelijke en voorafgaande toestemming nodig van de ontvanger. Wanneer je niet vooraf toestemming vraagt, maar je biedt wel gelegenheid om uit te schrijven, is dus onvoldoende.
Daarnaast geldt: ook al heb je toestemming, je moet ontvangers altijd een eenvoudige gelegenheid bieden tot uitschrijving voor zulke berichten door middel van een link onderaan de mailing of een tekst "Wanneer u in de toekomst geen mail van onze organisatie, kunt u dat door deze mail terug te sturen met de tekst: SVP mij uitschrijven voor uw mailingen."

Uitzondering voor nieuwsbrieven aan leden

Een uitzondering is het versturen van nieuwsbrieven en andere informatie over verenigingsactiviteiten aan leden. Een vereniging moet haar leden namelijk via e-mail kunnen informeren over het reilen en zeilen binnen de vereniging. Denk bijvoorbeeld aan de uitnodiging voor een ledenvergadering of de verenigingsevenementen, wedstrijduitslagen etc. Zolang een nieuwsbrief uitsluitend dergelijke berichten bevat, heb je geen uitdrukkelijke toestemming nodig van een lid.

Attentie: je moet de mailing dan wel uitsluitend richten aan leden, geen sponsors of adverteerders! Voor hen heb je namelijk wel toestemming vooraf nodig.

Zo'n nieuwsbrief mag geen ledenlijst bevatten. Ook hier geldt weer net als voor ledenlijsten op de website, toestemming vragen met duidelijke uitleg voor welk doel je die toestemming wilt gebruiken en uitsluitend naar leden mailen (geen sponsors, adverteerders etc.). Het is echter een donkergrijs gebied omdat zo'n mail weer makkelijk kan worden doorgestuurd naar ontvangers buiten de vereniging.

Let op

Een mailing mag geen ledenlijst of andere persoonsgegevens van leden of derden bevatten.
Voor het sturen van reclame (zoals sponsormailingen) aan leden heb je wél toestemming nodig.

Wanneer u als secretaris een mailing stuurt naar de leden mag u nooit die adressen in de velden Aan… of CC… plaatsen. Die moeten altijd staan in het veld BCC… zodat de ontvanger van de mailing nooit de mailadressen van de andere leden krijgt te zien en in het veld Aan… uw eigen mailadres.

Voorbeeld goed gebruik mailadressen:
Van… secretaris kleindiervereniging
Aan… secretaris kleindiervereniging
CC <leeg>
BCC… <mailadres lid 1>; <mailadres lid 2> etc.

Bij gewone, individueel gerichte mail mag u wel iemand in de CC zetten.

Catalogus

Vraag op het inschrijfformulier duidelijk om toestemming om de inzender in de inzenderslijst van de catalogus op te nemen en bewaar de inschrijfformulieren zorgvuldig. Gebruik bij digitale inschrijving een speciaal vinkje hiervoor en bewaar het. Bij geen toestemming …..???
Wij laten het aan de makers van tentoonstellingssoftware en webmodules voor inschrijvingen over hiervoor een technische oplossing te bedenken zodat de inzenderslijst alleen gegevens bevat van personen die expliciet toestemming hebben gegeven.

Een digitale catalogus op de website mag zeker geen inzenderslijst bevatten. Controleer of uw website oude catalogussen bevat en haal daar de inzenderslijst eruit.

Registers die u moet hebben en bijhouden

Er zijn drie registers die u moet bijhouden:
1. register verwerkingen door uzelf waarbij u verwerkersverantwoordelijk bent
2. logboek datalekken
3. register verwerkingen waarbij u een bewerker bent

Ad 1
Hierin moet u alle registraties van persoonsgegevens in opnemen, zoals de ledenadministratie etc.
Ad 2
Hierin moet u alle datalekken vermelden, ook die niet zijn gemeld. De gegevens van een datalek moeten drie jaar worden bewaard.
Ad 3
Dit is alleen van toepassing wanneer u de verwerking van persoonsgegevens doet voor een ander.

Bij deze brochure wordt een model meegestuurd.

Verwerking persoonsgegevens uitbesteed?

Het zal niet erg vaak voorkomen in onze hobby dat de verwerking van persoonsgegevens is uitbesteed. Een concreet voorbeeld is de inschrijvingen voor tentoonstellingen via een website die niet onder het beheer van uw vereniging valt.
Daarvoor heeft u een zgn. bewerkersovereenkomst nodig met de beheerder van die website.

Rechten van personen van wie de gegevens zijn geregistreerd

- Dataportabiliteit (gegevens kunnen overdragen naar een ander systeem)
- Recht op verwijdering van persoonsgegevens
- Inzage in de geregistreerde persoonsgegevens
- Rectificatie
- Beperking registratie
- Een menselijke blik bij besluiten bij geautomatiseerde beslissingen
- Bezwaar
- De informatieplicht van de AVG
- Mensen hebben recht op duidelijke informatie over wat u met hun persoonsgegevens doet (privacyverklaring)
- Wijs expliciet op de rechten van betrokkenen.

- Handel verzoeken binnen één maand en in begrijpelijke vorm af

Datalekken

Zie ook:
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens. We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens. Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.

Voorbeelden datalekken:
Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen of verloren laptop, een inbraak in een databestand door een hacker, uw computer is gegijzeld en er wordt om een betaling gevraagd.

Datalekken moeten binnen 72 uur worden gemeld aan de Autoriteit Persoonsgegevens. Als de situatie nog niet duidelijk is, mag eerst een deelmelding worden gedaan.

Waren niet alle gelekte gegevens (goed) versleuteld, of heeft het datalek om andere redenen waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene dan moet u dit ook melden aan betrokkene.

Niet alle datalekken hoeven te worden gemeld aan de Autoriteit Persoonsgegevens maar moeten wel in het register datalekken worden opgenomen.

Of u een datalek heeft en of u deze moet melden, kunt u afstemmen met de Autoriteit Persoonsgegevens zelf. Zie Tips en links voor het telefoonnummer. Maak daar gebruik van want zij zijn er voor u.

Aanstellen verantwoordelijke voor de AVG

U bent niet verplicht een zgn. functionaris voor de gegevensbescherming (FG) aan te stellen. Wel is het raadzaam om af te spreken hoe en wie toezicht houdt op de materie rondom de AVG en wie de meldingen datalekken gaat doen. Zorg ook voor vervangers ingeval van vakantie, uit de vereniging stappen e.d.
Zorg dat er hierover duidelijkheid is binnen uw organisatie.

Vrijwilligers en geheimhoudingsplicht

Verenigingen draaien van oudsher grotendeels op vrijwilligers. Deze vrijwilligers krijgen regelmatig toegang tot persoonsgegevens bij de uitoefening van hun taak. Denk bijvoorbeeld aan de toegang tot leden- en deelnemerslijsten. Je wil met zulke vrijwilligers begrijpelijkerwijs zo soepel mogelijk omgaan. Zo oefen je doorgaans minder uitdrukkelijk gezag uit dan bij werknemers, en zijn werkafspraken vaak minder strikt.
Vergeet echter nooit: vrijwillig betekent niet vrijblijvend! Een gebrek aan controle op vrijwilligers is vanuit privacy-opzicht niet zonder risico. De vereniging is als verantwoordelijke namelijk verplicht om

te bewaken dat vrijwilligers persoonsgegevens verwerken op de wijze zoals de vereniging voorschrijft. Schiet een vrijwilliger daarin tekort, dan kan dit in theorie leiden tot aansprakelijkheid van de vereniging en sancties van de toezichthouder. Stel daarom duidelijk beleid op, waarin je vrijwilligers uitlegt hoe zij met informatie van de vereniging moeten omgaan (geheimhoudingsplicht). Controleer bovendien af en toe of het beleid daadwerkelijk wordt nageleefd. Beperk ook de toegang tot persoonsgegevens, zodat vrijwilligers alleen toegang hebben tot gegevens die noodzakelijk zijn voor de uitvoering van hun taak.
Vrijwilligers kunnen soms plots uit beeld raken nadat zij hun taak neerleggen, of eenmalig assistentie hebben verleend. Vergeet dus nooit om tijdig de toegang tot informatie te beëindigen. Zorg ook dat alle persoonsgegevens worden teruggegeven, en waar nodig worden gewist van privéapparatuur van de vrijwilliger.

Maak duidelijke afspraken over geheimhoudingsplicht. Nog beter is om dit schriftelijk vast te leggen in een zgn. vrijwilligersovereenkomst.

Tips en links

Handige links zijn o.a.:
https://rvo.regelhulpenvoorbedrijven.nl/avg/welkom
https://veiliginternetten.nl/privacyverklaring-generator/start/
https://internet.nl/

U kunt voor uw vragen altijd terecht bij de Autoriteit Persoonsgegevens. De website bevat veel informatie en mocht u op de website het antwoord niet vinden, bel dan gerust naar het telefonisch spreekuur. Hou wel rekening met een langere wachttijd die kan oplopen tot meer dan 10 minuten.

- Het telefoonnummer is 088 - 1805 250.
- Bereikbaar: maandag t/m vrijdag van 9.00 tot 17.00 uur.
- U betaalt uw gebruikelijke telefoonkosten.

Bijlagen

Checklist privacyverklaring

Identiteit
De privacyverklaring dient de identiteit van de voor de verwerking verantwoordelijke te bevatten, inclusief fysieke en elektronische adresgegevens van uw organisatie.

Doeleinden
Een duidelijke uitleg waarom u de persoonsgegevens verzamelt en of bezoekers verplicht zijn deze gegevens te verstrekken. Bij doelen kunt u bijvoorbeeld denken aan: “de levering van een dienst”, “het beantwoorden van vragen van bezoekers”, “het versturen van nieuwsbrieven” of “het verzamelen van gegevens voor de analyse van de website”. Vermeld ook op basis van welke rechtsgrond de gegevens worden verwerkt. De meest voorkomende rechtsgronden zijn: “toestemming”, “wettelijke verplichting”, “uitvoeren overeenkomst” of “gerechtvaardigd belang”. Bij die laatste dient het betreffende gerechtvaardigde belang beschreven te worden. Een voorbeeld van een gerechtvaardigd (bedrijfs)belang is het gebruiken van contactgegevens van bestaande klanten voor het onder de aandacht brengen en aanbieden van nieuwe diensten.

Ontvangers
Als u persoonsgegevens van uw bezoekers ter beschikking stelt, of verkoopt, aan andere partijen, vermeld dat dan duidelijk.

Rechten betrokkenen
Wijs betrokkenen er in de verklaring op dat ze het recht hebben: om inzage, correctie of verwijdering te verzoeken van hun gegevens, bezwaar te maken tegen, of beperking te verzoeken van de verwerking van hun gegevens, toestemming in te trekken, hun gegevens over te dragen, een klacht in te dienen bij een toezichthoudende autoriteit. Vermeld tot wie betrokkenen zich kunnen wenden om deze rechten uit te oefenen.

Privacy vragen
Neem de contactgegevens (fysiek en elektronisch) van de dienst of persoon op die voor uw website verantwoordelijk is voor het beantwoorden van vragen over de bescherming van persoonsgegevens.

Cookies
Maakt de website gebruik van cookies, dan bent u verplicht uit te leggen welke cookies u gebruikt en wat u daarmee doet. Let er op dat u uw bezoekers om toestemming moet vragen voordat er cookies worden gebruikt, hierop zijn slechts enkele uitzonderingen. Overleg eventueel met de website leverancier om te achterhalen welke cookies (en vergelijkbare technieken) er worden gebruikt.

Automatische verzameling en besluitvorming
Indien van toepassing dient te worden toegelicht welke persoonsgegevens de website automatisch verzamelt. Denk hierbij bijvoorbeeld aan het vastleggen van IP-adressen van bezoekers in webserver logfiles voor analyse. Indien gebruik wordt gemaakt van automatische besluitvorming (waaronder profilering) dient dat vermeld te worden inclusief informatie over de onderliggende logica en de mogelijke gevolgen voor de betrokkenen. Profiling houdt in dat kantoren een profiel van mensen(bezoekers) opstellen door allerlei gegevens van hen te verzamelen, te analyseren en te combineren.

Beveiliging
Informatie over de technische en organisatorische maatregelen die zijn getroffen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.

Bewaartermijn

Vermeld hoelang u de verschillende persoonsgegevens gaat bewaren. Hou er rekening mee dat gegevens niet langer bewaard mogen worden dan nodig is voor de doeleinden waarvoor u ze hebt verzameld. Voor onbepaalde tijd bewaren mag niet zonder goede reden.

Uitsluiting

Licht, indien van toepassing, toe welke spelregels u hanteert voor het weigeren van toegang tot de website. Denk hierbij bijvoorbeeld aan het weigeren van bezoekers bij constatering van misbruik of oneigenlijk gebruik.