Implementatie Algemene verordening gegevensbescherming Huys Twickelo

Inhoud

1. Inleiding 3
2. Stappenplan 3
   - 2.1 Stap 1: Bewustwording 3
   - 2.2 Stap 2: Rechten van betrokkenen 3
   - 2.3 Stap 3: Overzicht verwerkingen 4
   - 2.4 Stap 4: Data privacy impact assessment (DPIA) 4
   - 2.5 Stap 5: Privacy by design & privacy by default 4
   - 2.6 Stap 6: Functionaris voor de gegevensbescherming 4
   - 2.7 Stap 7: Meldplicht datalekken 4
   - 2.8 Stap 8: Verwerkersovereenkomsten 4
   - 2.9 Stap 9: Leidende toezichthouder 4
   - 2.10 Stap 10: Toestemming 4
3. Implementatie VvE Huys Twickelo 5
   - 3.1 Stap 1: Bewustwording 5
   - 3.2 Stap 2: Rechten van betrokkenen 5
   - 3.3 Stap 3: Overzicht verwerkingen 5
   - 3.4 Stap 4: Data privacy impact assessment (DPIA) 7
   - 3.5 Stap 5: Privacy by design & privacy by default 7
   - 3.6 Stap 6: Functionaris voor de gegevensbescherming 7
   - 3.7 Stap 7: Meldplicht datalekken 7
   - 3.8 Stap 8: Verwerkersovereenkomsten 8
   - 3.9 Stap 9: Leidende toezichthouder 8
   - 3.10 Stap 10: Toestemming 8

1. Inleiding

Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat er vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.

De AVG is ook wel bekend onder de Engelse naam: General Data Protection Regulation (GDPR).

De AVG versterkt de positie van de betrokkenen (de mensen van wie gegevens worden verwerkt). Zij krijgen nieuwe privacyrechten en hun bestaande rechten worden sterker. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De nadruk ligt op de verantwoordelijkheid van organisaties om te kunnen aantonen dat zij zich aan de wet houden.

Dat geldt ook voor Verenigingen van Eigenaren en dus ook voor VvE Huys Twickelo.
In dit document wordt behandeld welke maatregelen VvE Huys Twickelo neemt om de Algemene verordening gegevensbescherming te implementeren. Dat gebeurt aan de hand van een 10-stappenplan zoals gepubliceerd door de Autoriteit Persoonsgegevens.

2. Stappenplan

Het stappenplan omvat de volgende onderdelen. Niet elk onderdeel hoeft door elke organisatie te worden geïmplementeerd. Dat is afhankelijk van het type organisatie.

- Stap 1: Bewustwording
- Stap 2: Rechten van betrokkenen
- Stap 3: Overzicht verwerkingen
- Stap 4: Data privacy impact assessment (DPIA)
- Stap 5: Privacy by design & privacy by default
- Stap 6: Functionaris voor de gegevensbescherming
- Stap 7: Meldplicht datalekken
- Stap 8: Verwerkersovereenkomsten
- Stap 9: Leidende toezichthouder
- Stap 10: Toestemming

2.1 Stap 1: Bewustwording

In deze fase moet ervoor worden gezorgd dat de relevante mensen in de organisatie op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op de huidige processen en diensten, en welke aanpassingen nodig zijn om aan de AVG te voldoen.

2.2 Stap 2: Rechten van betrokkenen

Onder de AVG krijgen betrokkenen (in ons geval wil dat zeggen, de eigenaren) meer en verbeterde privacyrechten. Daarom moet ervoor worden gezorgd dat zij hun privacyrechten goed kunnen uitoefenen.
Daarbij gaat het om bestaande rechten, zoals het recht op inzage en het recht op correctie en verwijdering. Maar ook nieuwe rechten, zoals het recht op dataportabiliteit. Bij dit recht moet ervoor worden gezorgd dat betrokkenen hun gegevens makkelijk kunnen krijgen en vervolgens kunnen doorgeven aan een andere organisatie als ze dat willen.
Ook kunnen mensen klachten indienen bij de AP (Autoriteit Persoonsgegevens) over de manier waarop met hun gegevens wordt omgegaan. De AP is verplicht deze klachten te behandelen.

2.3 Stap 3: Overzicht verwerkingen

De gegevensverwerkingen moeten in kaart worden gebracht. Er moet documentatie zijn van welke persoonsgegevens verwerkt worden en met welk doel dit gedaan wordt, waar deze gegevens vandaan komen en met wie ze gedeeld worden.

2.4 Stap 4: Data privacy impact assessment (DPIA)

Onder de AVG kan het verplicht zijn een zogeheten data protection impact assessment (DPIA) uit te voeren, waarmee vooraf de privacyrisico's van de gegevensverwerking in kaart worden gebracht. Dat is alleen van toepassing als het gaat om privacygevoelige informatie, niet wanneer het bijvoorbeeld uitsluitend om contactinformatie gaat.
Wel moet worden vastgelegd welke maatregelen worden genomen om de risico's te verkleinen.

2.5 Stap 5: Privacy by design & privacy by default

Privacy by design houdt in dat al bij het ontwerpen van diensten ervoor wordt gezorgd dat persoonsgegevens goed worden beschermd en dat niet meer gegevens worden verzameld dan noodzakelijk voor het doel van de verwerking. En ook dat gegevens niet langer worden bewaard dan nodig is.
Privacy by default houdt in dat er technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat standaard alléén persoonsgegevens worden verwerkt die noodzakelijk zijn voor het specifieke doel.

2.6 Stap 6: Functionaris voor de gegevensbescherming

Onder de AVG kan het verplicht zijn om een functionaris voor de gegevensverwerking (FG) aan te stellen. Dat is vooral van toepassing voor organisaties die persoonsgegevens analyseren (profiling) en wanneer bijzondere persoonsgegevens worden opgeslagen.

2.7 Stap 7: Meldplicht datalekken

De AVG stelt strengere eisen aan de registratie van de datalekken die zich hebben voorgedaan. Alle datalekken moeten worden gedocumenteerd. Met deze documentatie moet de AP kunnen controleren of aan de meldplicht is voldaan.

2.8 Stap 8: Verwerkersovereenkomsten

Is de gegevensverwerking uitbesteed aan een verwerker?
Er moet dan worden beoordeeld of de overeengekomen maatregelen in bestaande contracten nog toereikend zijn. En of deze voldoen aan de eisen die de AVG aan verwerkersovereenkomsten stelt.

2.9 Stap 9: Leidende toezichthouder

Dit is van toepassing als er vestigingen in meerdere EU-lidstatenzijn of als de gegevensverwerkingen in meerdere lidstaten impact hebben. In dat geval wordt er één privacytoezichthouder aangewezen. Dit wordt de leidende toezichthouder genoemd.

2.10 Stap 10: Toestemming

Voor sommige gegevensverwerkingen is toestemming nodig van de betrokkenen. De AVG stelt strengere eisen aan toestemming. Aangetoond moet worden dat geldige toestemming van mensen is verkregen om hun persoonsgegevens te verwerken. Ook moet het voor mensen net zo makkelijk zijn om hun toestemming in te trekken als om die te geven.

3. Implementatie VvE Huys Twickelo

Hierna wordt per stap aangegeven wat VvE Huys Twickelo doet om te voldoen aan de regels van de AVG.

3.1 Stap 1: Bewustwording

Hoewel bewustwording binnen de regels van de AVG uitgelegd kan worden als vooral geldend voor het bestuur, zal ook aan de leden uitleg gegeven worden, d.m.v. een publicatie op het publicatiebord, dat er nieuwe wetgeving van kracht wordt betreffende de privacy van de leden en wat de vereniging doet om de gegevens die zij van de leden bewaart, te beschermen.

3.2 Stap 2: Rechten van betrokkenen

De leden krijgen inzage in de gegevens die bewaard worden. Daarbij gaat het in eerste instantie alleen om NAW-gegevens en daarnaast enkele aanvullende gegevens, zoals bankrekeningnummer, afgegeven bankmachtigingen, e-mailadres, telefoonnummer.
Tevens zal hen de mogelijkheid geboden worden om die gegevens waar mogelijk te corrigeren.

3.3 Stap 3: Overzicht verwerkingen

De volgende persoonsgegevens van de leden zijn opgeslagen:

- Titel.
  De manier waarop het lid wordt aangesproken.
  De volgende opties zijn mogelijk: *heer*, *mevrouw, heer en mevrouw*.
- Voorletters.
  Behoeft geen nadere uitleg.
- Voorvoegsel.
  Bijvoorbeeld "*van*" of "ter" of "*ten*".
- Achternaam.
  De achternaam van het lid.
- Instantie.
  Dit veld wordt ingevuld met de naam van een instantie die het beheer namens een lid uitvoert.
- Adres.
  Alleen de straatnaam of bijv. "Postbus"
- Nummer
  Het huisnummer of postbusnummer.
- Postcode.
  Behoeft geen nadere uitleg.
- Woonplaats.
  Behoeft geen nadere uitleg.
- E-mail.
  Het E-mail adres. Wordt gebruikt bij verzending van mededelingen en servicemails.
- Indicator mededelingen via e-mail
  Geeft aan of men ook via e-mail de publicaties op het publicatiebord toegestuurd wil krijgen.
- IBAN Rekeningnummer.
  Het bankrekeningnummer bestaande uit 18 tekens.
  Wordt gebruikt bij het uitvoeren van incasso's.
- BIC nummer.
  Wordt gebruikt bij het uitvoeren van incasso's.
- Telefoonnummer.
  Behoeft geen nadere uitleg.
- Datum begin lidmaatschap.
  Is informatief en is niet voor alle leden ingevuld.

- Datum einde lidmaatschap.
  Wordt gebruikt in verschillende overzichten om te bepalen of de gegevens van dit lid nog actueel zijn.
- Machtiging afgegeven servicekosten.
  Geeft aan of het lid een machtiging heeft afgegeven voor incasso van de servicekosten en collectieve contracten.
- GEAS Contract.
  Indicator die aangeeft of, en zo ja welk, GEAS contract door het lid is afgesloten.
- Collectief contract.
  Soms wordt een collectief contract afgesloten voor onderhoud aan installaties die aanwezig zijn bij een meerderheid van de bewoners. Hier wordt aangegeven of het betreffende lid heeft aangegeven deel te willen nemen aan zo'n collectief contract.

Verder worden ten behoeve van de financiële administratie de volgende gegevens per lid bewaard:
- Bankmachtigingen
  - Soort bankmachtiging, doorlopend of eenmalig
  - Datum ondertekening
  - Identificatie bankmachtiging
  - Reden afgifte machtiging
- Incasso-opdrachten
  - Omschrijving van de opdracht
  - Betalingskenmerk
  - Bedrag

  Alle incasso-opdrachten sinds 1 januari 2005 zijn in het systeem opgeslagen, voor zover het huidige leden betreft.

Voor enkele functionarissen binnen de vereniging is het mogelijk om gemaakte onkosten te declareren.
Van declaraties wordt het volgende in de database opgeslagen:
- Identificatie van het lid
- Datum indienen declaratie
- Indicator uitbetaling
- Onkostenspecificatie bestaande uit:
  - Omschrijving
  - Bedrag

Voor alle informatie geldt dat deze is opgeslagen in een database op internet op een beveiligde server.
Tevens is er een kopie-database op een harddisk op de PC van de secretaris, de heer Meijer. Deze kopie is er om twee redenen:
- Als back-up
- Ten behoeve van het verzenden van fysieke post aan de leden.
  Opties van MS-Word worden gebruikt om adresgegevens uit de database te halen en deze in de brieven in te voegen.

Daarnaast zijn er fysieke mappen met de oorspronkelijke aanmeldingsgegevens en de oorspronkelijke bankmachtigingen.

Met sommige bedrijven is een collectief contract afgesloten ten behoeve van onderhoud en/of reparatie van bij de leden aanwezige installaties. Aan die contractanten zijn alleen NAW-gegevens van de deelnemers verstrekt.

Alle persoons gerelateerde gegevens zullen worden bewaard gedurende de tijd dat het lidmaatschap van de vereniging loopt. Na afloop van het lidmaatschap zullen alle gegevens nog 2 jaar bewaard blijven.

3.4 Stap 4: Data privacy impact assessment (DPIA)

Er zal geen assessment worden uitgevoerd.
Wel zijn er maatregelen genomen om toegang tot de opgeslagen gegevens te beveiligen.
Alle gegevens in de database op internet staan op een beveiligde server en deze gegevens zijn slechts toegankelijk via een beveiligde verbinding (SSL).
Twee personen in de organisatie hebben toegang tot alle gegevens en kunnen d.m.v. een voor dat doel ontwikkeld administratieprogramma die gegevens ook wijzigen. Dat zijn:

- De secretaris, de heer Meijer
- De penningmeester, de heer Wienk

Zij krijgen die toegang na het invoeren van een gebruikersnaam en een alleen bij hen bekend wachtwoord.
Alle leden van de vereniging hebben, d.m.v. een door hen aangevraagde beveiligde toegang tot de website van de vereniging, ook toegang tot informatie als een bewonerslijst, een eigenarenlijst, notulen van ledenvergaderingen en financiële jaarverslagen. Die toegang wordt verkregen na het invoeren van een gebruikersnaam en een alleen bij dat lid bekend wachtwoord.

De fysieke mappen met de oorspronkelijke papieren aanmeldingsgegevens en de oorspronkelijke papieren bankmachtigingen staan in een kast ten huize van de secretaris en is slechts toegankelijk voor die persoon.
Daarnaast zullen alle leden, mits zij kenbaar gemaakt hebben dat te willen, via de website van de vereniging toegang krijgen tot hun eigen persoonlijke gegevens en kunnen zij die desgewenst corrigeren.

3.5 Stap 5: Privacy by design & privacy by default

- Privacy by design
  Alle gegevens zijn beschermd d.m.v. opslag op een beveiligde server en toegang d.m.v. een beveiligde verbinding.
- Privacy by default
  In het datamodel zijn alléén die gegevens opgenomen die noodzakelijk zijn voor het voeren van een correcte administratie.

3.6 Stap 6: Functionaris voor de gegevensbescherming

Er zal geen functionaris voor gegevensbescherming worden aangesteld.
In onze organisatie lijkt dat niet nodig, omdat er geen sprake is van het analyseren van persoonsgegevens en er ook geen bijzondere persoonsgegevens worden opgeslagen.

3.7 Stap 7: Meldplicht datalekken

We spreken van een datalek als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben.
Een datalek is het gevolg van een beveiligingsprobleem.
Het kan dan gaan om uitgelekte computerbestanden of een geprint overzicht dat in verkeerde handen is gekomen. Andere voorbeelden zijn cyberaanvallen, verkeerd verzonden e-mail, gestolen laptops, afgedankte niet-schoongemaakte computers en verloren usb-sticks.
De procedure na het ontstaan en ontdekken van een datalek uit de volgende stappen:

- Het lek moet gemeld worden bij een daarvoor aangewezen persoon in de organisatie. Nog niet afgesproken is wie in de organisatie moet worden.
- In kaart gebracht moet worden wat de gevolgen zijn voor de personen van wie persoonsgegevens gelekt zijn.
- Meldingen moeten vervolgens gedaan worden bij de Autoriteit Persoonsgegevens.
  De melding moet in ieder geval bestaan uit:
  - de aard van de inbreuk;

- de instanties of persoon 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 de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens;
- de maatregelen die zijn genomen of worden voorgesteld te nemen om deze gevolgen te verhelpen.

- De aangewezen persoon doet vervolgens de melding digitaal bij het meldloket van de Autoriteit Persoonsgegevens: http://datalekken.autoriteitpersoonsgegevens.nl.

3.8 Stap 8: Verwerkersovereenkomsten

Is niet van toepassing, aangezien alle verwerking gebeurt in eigen beheer.

3.9 Stap 9: Leidende toezichthouder

Is niet van toepassing omdat er maar één vestiging is.

3.10 Stap 10: Toestemming

Aan alle leden zal een overzicht worden gestuurd van de persoonsgegevens die van hen zijn opgeslagen. Daarbij zal hen worden gevraagd om die gegevens te controleren en daar waar nodig te corrigeren of aan te vullen. Door retourzending van (gecorrigeerde) formulieren wordt tevens toestemming verleend voor opslag van die gegevens.

Aangezien het bestuur verplicht is een correcte ledenadministratie te voeren, is expliciete toestemming niet nodig, althans niet voor die gegevens die noodzakelijk zijn voor het voeren van een correcte administratie, maar in de begeleidende brief zal worden gemeld dat niet-gecorrigeerde gegevensformulieren worden beschouwd als toestemming voor opslag van de betreffende gegevens.