Handreiking omgaan AVG voor deelnemers hierkomjijweg

Inleiding

Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing, uitgevoerd door de Autoriteit Persoonsgegevens (AP). De belangrijkste doelstelling van de AVG is dat de privacyrechten van mensen vergroot en versterkt worden. De AVG gaat over het omgaan met bijzondere persoonsgegevens: '*alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon*'. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Gegevens van overleden personen of van organisaties zijn geen persoonsgegevens volgens de AVG.

In deze notitie wordt een korte uitleg gegeven over de wet, maar vooral een handreiking geboden hoe kleine organisaties met de nieuwe verordening om kunnen gaan. Als iemand er om vraagt moet een organisatie kunnen aangeven welke gegevens de organisatie van een persoon heeft. Deze gegevens moeten ook beschermd worden. Er mogen gegevens bewaard worden, maar bij alles moet nagegaan worden waarom welke gegevens bewaard worden, en hoelang.

Wanneer mag ik gegevens verwerken?

Je moet aan kunnen tonen waarom je persoonlijke gegevens verwerkt. De AP kent zes grondslagen, waarbij je aan minimaal één grondslag moet voldoen:
- Toestemming van de betrokken persoon;
- De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst;
- De gegevensverwerking is noodzakelijk voor het nakomen van een wettelijke verplichting;
- De gegevensverwerking is noodzakelijk ter bescherming van de vitale belangen;
- De gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag;
- De gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen.

Hoe zorg je dat je organisatie voldoet aan de AVG? Van alle organisaties wordt een actieve houding verwacht. Door alles omtrent persoonsgegevens bij te houden en van tevoren vast te leggen waarom je welke gegevens nodig hebt wordt men bewust van de privacy van anderen. Daarnaast moeten alle organisaties ook zorgen dat alle banden die men heeft met andere organisaties ook aan de wet voldoen. Je sluit verwerkersovereenkomsten af met bijvoorbeeld het ICT-bedrijf die de computers beheerd.

Hoe kan je nu aantonen aan de AP dat je aan je plichten hebt voldaan? Daarvoor kan je een aantal dingen doen. Als je aan al deze punten voldoet is je organisatie behoorlijk AVG-proof. Als organisatie hoef je niet morgen aan al deze eisen te voldoen. Het is echter wel van belang dat er binnen de organisatie gewerkt wordt aan het belang van privacy, en dat je dit ook kan aantonen.

1. Verwerkingen persoonsgegevens

Verwerkingsverantwoordelijke en verwerker: Een verwerkingsverantwoordelijke bepaalt volgens de AVG het doel en het middel van de verwerking (waarom en hoe). Een verwerker is een externe partij (dus geen werknemer/vrijwilliger van de verantwoordelijke) die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Plichten verwerkingsverantwoordelijke
- Rechtmatig, behoorlijk en transparant werken
- Doelgebonden verwerken
- Slechts met minimaal noodzakelijke gegevens werken
- Juiste gegevens verwerken
- (Verwerkte) gegevens blijven beperkt opgeslagen
- Gegevens worden integer en vertrouwelijk behandeld en goed beveiligd.

Plichten verwerker
- Handelt alleen in opdracht van de verwerkingsverantwoordelijke
- Houdt de verwerkte categorieën persoonsgegevens bij in een register
- Neemt beveiligingsmaatregelen passend bij de gegevensverwerking
- Vraagt verwerkingsverantwoordelijke toestemming voor subverwerkingen
- Meldt datalekken
- Verleent medewerking aan Autoriteit Persoonsgegevens
- Stelt een Functionaris Gegevensbescherming aan in het geval van overheids- of publieke organisaties, verwerken van grootschalige persoonsgegevens of bij observaties. Veel organisaties hebben beide rollen.

Verwerkingsregister: register met alle verwerkingen van persoonsgegevens.

Verwerkersovereenkomsten: opstellen van verwerkersovereenkomsten met verwerkers waarin je alle plichten vastlegt. De verwerkingsverantwoordelijke is aan zet.

Procedure grondslag toestemming: documenteren van de wijze waarop u toestemming vraagt en het bewijs dat de toestemming is gegeven.

Procedure grondslag gerechtvaardigd belang: documenteren van gerechtvaardigd belang

Procesdocumenten: documenteren van de processen om de rechten van de betrokkenen te waarborgen

2. Datalekken

Procedures omgang datalekken: documenteren van de procedure omtrent datalekken, na kennisneming van het datalek moet binnen 72 uur melding gemaakt worden aan AP, bij hoog risico voor de betrokkene, ook melden aan de betrokkene.

Datalekkenregister: bijhouden van datalekken die zich hebben voorgedaan in een register (feiten en gegevens over de aard; categorieën persoonsgegevens; aantal betrokkenen, gevolgen; genomen maatregelen; melding aan AP; melding aan betrokkenen).

3. Privacy

Gegevensbeschermingsbeleid/Privacybeleid: opstellen van een passend gegevensbeschermingbeleid met daarin: Categorieën persoonsgegevens voor verwerking; doeleinden van de verwerking; bewijslast te voldoen aan de beginselen van verwerking van persoonsgegevens (bijv. dataminimalisatie); rechten van de betrokkenen en hoe zij die rechten kunnen uitoefenen; de genomen organisatorische en technische maatregelen om de persoonsgegevens te beveiligen; bewaartermijn van persoonsgegevens.

Privacy statement: Vastleggen van informatievoorzieningen aan de betrokkenen, deze ook publiceren op de website (eventueel met bijbehorende privacybeleid en -reglement).

4. Gegevensbescherming

Privacy by design: Privacy onder de aandacht vanaf de ontwerpfase tot de afrondingsfase van een project.

Privacy by default: Technische en organisatorische maatregelen waarbij standaard alleen noodzakelijke persoonsgegevens worden verwerkt (bijvoorbeeld bij het aanmelden op een website het vakje 'ja, ik wil aanbiedingen ontvangen' standaard uit te zetten).

Gegevensbeschermingseffectbeoordelingen: Documenteren van beoordelingen van de risico's op gegevensbescherming bij nieuwe verwerkingen met hoge risico's, ook wel Data Privacy Impact Assessment (DPIA) genoemd. Een dergelijke beoordeling geeft inzicht in de impact en risico's van het beoogde project op de privacy van de betrokkene.

Functionaris Gegevensbescherming (FG): De FG houdt toezicht op de naleving van de AVG binnen de organisatie. De FG is verplicht in geval van overheid, verwerking bijzondere persoonsgegevens en bij observatie (bijv. cameratoezicht). Wanneer onduidelijk is of u verplicht bent om een FG aan te stellen, moet u goed kunnen onderbouwen waarom u ervoor gekozen hebt om dat wel of niet te doen.

5. Betrokken

Informatieplicht: De verwerkingsverantwoordelijke moet de betrokkene informeren over hoe hij omgaat met de verzamelde persoonsgegevens. De privacyverklaring, - beleid, en – reglement moeten op de website gepubliceerd en voor de betrokkene terug te vinden zijn.

Recht op gegevenswissing en dataportabiliteit: organisaties moeten persoonsgegevens op verzoek verstrekken aan betrokkene, en op verzoek gegevens verwijderen.

Welke documenten moet mijn organisatie hebben?

Een aantal documenten kunnen binnen de organisatie binnen het kader van de AVG niet ontbreken.

- Verwerkingsregister: Hierin staan alle activiteiten die je als organisatie doet met betrekking tot persoonsgegevens. Ook staat hierin welke gegevens dat dan zijn, waarom je ze nodig hebt, en hoelang je ze bewaart als je ze niet meer nodig hebt.
- Datalekkenregister
- Gegevensbeschermingsbeleid/Privacybeleid
- Gegevensbeschermingseffectbeoordelingen (DPIA)
- Privacy statement
- Procedure grondslag gerechtvaardigd belang (alleen van toepassing bij hantering grondslag)
- Procedure grondslag toestemming (alleen van toepassing bij hantering grondslag)
- Procedures omgang datalekken
- Procesdocumenten
- Verwerkersovereenkomsten

Omgaan met (publicatie van) bronnen

Wat betekent de AVG nu voor de publicatie van je bronmateriaal? Er zit een verschil tussen beeldmateriaal van personen en persoonsgegevens. Het maken van foto- en videobeelden met herkenbaar in beeld gebrachte personen is een verwerking van persoonsgegevens en mag in principe niet verwerkt worden op basis van de AVG. Dit is echter niet van toepassing tenzij aan voorwaarden voldaan wordt. In dit geval is de verwerking noodzakelijk met het oog op archivering in algemeen belang, wetenschappelijk en historisch onderzoek (behoud en presentatie van het cultureel erfgoed).

Beeldmateriaal in de huidige databases op Hierkomjijweg is dermate zo omvangrijk dat het niet evenredig is om met terugwerkende kracht uitdrukkelijke toestemming te vragen aan betrokkenen en hun databases daarop aan te passen (let op: hierbij gaat het niet over het auteursrecht). Vraag toestemming bij het ontvangen van nieuw beeldmateriaal.

Wanneer iemand bezwaar maakt op het huidige gepubliceerde beeldmateriaal, onderneem dan actie door bijvoorbeeld de naam en/of andere gegevens te verwijderen of te anonimiseren. In een persoonlijke administratie kan de naam bewaard blijven (historisch onderzoek). Ga nieuw beeldmateriaal pseudonimiseren (ontkoppel de naam en adres etc. van de foto zelf, eventueel anonimiseren in bepaalde gevallen).