Algemene Verordening Gegevensbescherming
Voor erfgoed organisaties

Inhoud

Inleiding

Vanaf 25 mei 2018 is de Europese Algemene verordening gegevensbescherming (“*AVG*”) van kracht. In de hele Europese Unie geldt dan dezelfde privacywetgeving. De huidige Wet bescherming persoonsgegevens (Wbp) is vanaf dat moment niet meer geldig.

De AVG:

- legt meer verantwoordelijkheden bij de organisatie die persoonsgegevens verwerkt (“verwerkingsverantwoordelijke”)
- beschermt en versterkt de rechten van de personen van wie persoonsgegevens worden verwerkt (“betrokkenen”)
- geeft de toezichthouder, de Autoriteit Persoonsgegevens, meer bevoegdheden, waaronder de bevoegdheid om hoge boetes op te leggen.

Deze verordening geldt voor alle organisatie, dus ook voor verenigingen, stichtingen, koepelorganisaties.

Christa van der Aa, 26-4-2018

Algemene Verordening Gegevensbescherming
Voor erfgoed organisaties

Enkele belangrijke begrippen in het kader van de AVG

Persoonsgegevens

De Wet bescherming persoonsgegevens (Wbp) geeft aan dat een persoonsgegeven elk gegeven is over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Dat het om een natuurlijke persoon moet gaan, houdt in dat gegevens van overleden personen of van organisaties geen persoonsgegevens zijn.

Foto's en beeldmateriaal zijn vaak ook persoonsgegevens. Als de foto's direct of indirect herleidbaar zijn tot een persoon, dan zijn het persoonsgegevens.

We raden aan om alle gegevens waarvan je vermoedt dat die herleidbaar zijn tot een persoon te behandelen alsof het persoonsgegevens zijn.

Bijzondere persoonsgegevens

Dit zijn gegevens over iemands godsdienst of levensovertuiging, ras, politieke voorkeur, gezondheid, seksuele leven, lidmaatschap van een vakbond, strafrechtelijk verleden. Ook het burgerservicenummer (BSN) is een bijzonder persoonsgegeven, omdat het een uniek en tot de persoon herleidbaar nummer is.

Een organisatie mag geen bijzondere persoonsgegevens gebruiken, tenzij daarvoor in de wet een uitzondering is. De uitzonderingen vind je op de website van de Autoriteit Persoonsgegevens.

Verwerken

Alle handelingen die een organisatie kan uitvoeren met persoonsgegevens, van verzamelen tot en met vernietigen wordt gezien als verwerken.

Dit is dus een zeer ruim begrip. Handelingen die er volgens de Wet bescherming persoonsgegevens (Wbp) in ieder geval onder vallen, zijn: het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

De verwerkingsverantwoordelijke

De verwerkingsverantwoordelijke is een persoon of een organisatie die het doel van en de middelen voor het gebruik van persoonsgegevens bepaalt. De verantwoordelijke kan dit alleen doen of samen met anderen. Het houdt in dat de verantwoordelijke uiteindelijk beslist of een organisatie persoonsgegevens verwerkt, en zo ja:

- om welke verwerking het gaat;
- welke persoonsgegevens de organisatie hierbij verwerkt;
- voor welk doel de organisatie dit doet;
- op welke manier de organisatie dit doet.

De betrokkene

De betrokkene is degene van wie een organisatie persoonsgegevens verwerkt. Dit is dus degene op wie de persoonsgegevens betrekking hebben.

Algemene Verordening Gegevensbescherming
Voor erfgoed organisaties

Een verwerker
Een verwerker is een persoon of organisatie aan wie de verantwoordelijke de gegevensverwerking heeft uitbesteed. Bijvoorbeeld een administratiekantoor.

Een verwerker is niet zelfstandig verantwoordelijk voor de verwerking van de persoonsgegevens. Maar de verwerker heeft wel een aantal afgeleide verplichtingen, voor onder meer beveiliging en geheimhouding van de gegevens.

Wettelijke grondslagen
Als organisatie mag je niet zomaar persoonsgegevens verwerken. Je moet daarvoor een wettelijke grondslag hebben. De Algemene verordening gegevensbescherming (AVG) kent 6 grondslagen.

Kun je de gegevensverwerking niet baseren op minimaal één van deze grondslagen? Dan heb je niet het recht om de persoonsgegevens te verwerken. De 6 grondslagen voor het verwerken van persoonsgegevens:

- Toestemming van de betrokken persoon.
- De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst.
- De gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen.
- 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.

Bij noodzakelijk voor de uitvoering van de overeenkomst is belangrijk dat de overeenkomst niet uitgevoerd kan worden zonder die persoonsgegevens. Denk bijvoorbeeld aan de ledenadministratie waarbij een naam, adres en bijvoorbeeld emailadres nodig is. Is het verwerken van de persoons-gegevens alleen maar handig, maar niet noodzakelijk, dan kan deze grondslag niet gebruikt worden.

Het gerechtvaardigd belang is vooral een belangenafweging. De verwerking moet noodzakelijk zijn voor de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde, tenzij de privacybelangen van de betrokkene zwaarder wegen. Hierbij moet bijvoorbeeld rekening gehouden worden met de vraag in hoeverre de betrokkene had mogen verwachten dat de verwerking plaats zou vinden en met welk doel dan. Dit belang kan bijvoorbeeld gebruikt worden om direct marketing mogelijk te maken. Let wel op dat een betrokkene altijd bezwaar mag maken tegen direct marketing en de verwerking dan moet stoppen. Het gerechtvaardigd belang is ook belangrijk voor fotografen die bijvoorbeeld fotograferen op evenementen, journalistieke of documentaire fotografie verzorgen waarbij een quitclaim niet mogelijk is of wanneer het gaat om straatfotografie.

Datalek
Een inbreuk in verband met persoonsgegevens, beter bekend als een datalek, is een inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.
In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht.
Wanneer je hebt vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dien je ook aan de betrokkenen te melden dat er sprake is geweest van een inbreuk in verband met persoonsgegevens.
Christa van der Aa, 26-4-2018

Algemene Verordening Gegevensbescherming
Voor erfgoed organisaties

Welke stappen kun je ondernemen om AVG proof te zijn?
Hieronder een aantal stappen waarmee je je goed voorbereidt op de vereisten van de AVG. Er staan ook wat tips die je kunnen helpen bij de stappen.

Stap 1 zorg voor bewustwording
Het is belangrijk dat iedereen binnen je organisatie weet dat de nieuwe AVG van toepassing is en wat de gevolgen zijn. Van het bestuur (of de directie), tot en met alle medewerkers en vrijwilligers die persoonsgegevens verwerken (bijvoorbeeld gebruiken of kunnen inzien).

Vrijwilligers informeren of opleiden
Het is niet de bedoeling dat wanneer je de gegevensbescherming zorgvuldig in beleid en procedures hebt geregeld, vrijwilligers met persoonsgegevens die nodig zijn bij de uitoefening van zijn/haar functie, te koop gaat lopen. Dat zijn namelijk datalekken. Dit kan gaan om gegevens uit de bestanden van de organisatie zelf, maar ook om informatie die een vrijwilliger van een deelnemer of ouder heeft gekregen.

DOEN

We adviseren om één persoon binnen je organisatie of binnen het bestuur aan te wijzen die verantwoordelijk is voor de correcte verwerking van de persoonsgegevens. Hij/zij zal samen met het bestuur, moeten inschatten wat de impact van de AVG is voor het huidige gebruik van de persoonsgegevens en de processen binnen je organisatie. Deze verantwoordelijke zal ook moeten onderzoeken welke aanpassingen nodig zijn.

Geef in een nieuwsbrief of tijdens een bijeenkomst uitleg over de AVG en nodig mensen uit om mee te helpen bij de activiteiten om te voldoen aan de AVG. Bijvoorbeeld bij de inventarisatie.

Stap 2 Inventariseer waarom, hoe en wat
Onder de AVG heeft je organisatie een zogenaamde ‘verantwoordingsplicht’. Dit houdt in dat jullie altijd moeten kunnen aantonen dat je organisatie handelt in overeenstemming met de AVG.
Je bent verplicht te inventariseren wat je vastlegt én te registreren hoe je dat doet. Bovendien mag je alleen persoonsgegevens vastleggen als dat functioneel is. Dit houdt in dat je alleen persoonsgegevens vastlegt die je nodig hebt en dat je ze alleen gebruikt waarvoor je ze verzamelt. Bovendien mag je ze niet langer bewaren dan nodig.

Begin daarom met het in kaart brengen en documenteren van de persoonsgegevens die jullie momenteel verwerken. Vervolgens kunnen jullie beoordelen wat er moet gebeuren om aan de AVG te voldoen.

DOEN

Breng de verwerking van de persoonsgegevens in kaart door de volgende informatie te verzamelen:

Wat?
- welke persoonsgegevens verwerken jullie?
  zoals naam, adres, bankgegevens, telefoonnummer, geslacht, e-mailadres

- van welke categorieën betrokkenen zijn de persoonsgegevens?
  zoals leden, donateurs, vrijwilligers, personeelsleden
- verwerken jullie ook gegevens over gezondheid of andere bijzondere persoonsgegevens?
  zoals aandoening, medicijngebruik, religieuze of levensbeschouwelijke overtuigingen

Waarom?

- voor welk doel gebruiken jullie de persoonsgegevens?
  zoals innen lidmaatschapsgeld, verzenden van informatie, uitnodigingen bijeenkomsten

Hoe?

- Hoe verzamelen jullie de gegevens? Wat is de bron?
- Vragen jullie toestemming voor de verwerking? Of is er sprake van een andere wettelijke grondslag?
- Op welke manier kunnen jullie bewijzen dat je toestemming hebt voor de verwerking van de persoonsgegevens, gebruik van foto's, films e.d.
- Gebruiken jullie een privacyverklaring of hebben jullie andere informatie aan de betrokkenen verstrekt?
- Wie hebben er allemaal toegang tot de persoonsgegevens?
  bijvoorbeeld welke personeelsleden, vrijwilligers, andere derden (verwerkers)?
- Hebben jullie met deze derden/verwerkers een verwerkersovereenkomst gesloten?
- Hoe worden de persoonsgegevens beveiligd / is er een beveiligingsbeleid?
- Hoe lang worden de persoonsgegevens bewaard?

Met deze informatie zullen jullie moeten inschatten welke stappen de organisatie nog moet zetten om te voldoen aan de AVG.

TIP 1 Wat is "verwerken"?

Het begrip 'verwerken' is zeer breed. In feite is iedere handeling met een persoonsgegeven een verwerking. Denk dus aan het verzamelen, opslaan, bewaren, verplaatsen, wissen, doorsturen of aanpassen, maar ook aan het kwijtraken van persoonsgegevens. In dat laatste geval spreek je van een 'datalek'.

Tip 2 Dataminimalisatie

De AVG gaat uit van dataminimalisatie. Dit betekent dat organisaties zo min mogelijk persoonsgegevens moeten verwerken en uitsluitend die gegevens die nodig zijn voor het te bereiken doel. Vraag je bij alle te verwerken persoonsgegevens af of deze gegevens echt noodzakelijk zijn voor het doel dat jullie nastreven.
Bewaar gegevens ook niet langer dan ze nodig zijn voor de verwerking. Het is verleidelijk om de gegevens vast te houden 'voor het geval dat' het nuttig is, maar naarmate de informatie ouder wordt, wordt het minder een voordeel en meer een risico.

TIP 3 Bijzondere persoonsgegevens

De AVG legt extra verplichtingen op aan organisaties die gegevens verwerken over de bijzondere persoonsgegevens. Het gaat specifiek om: gegevens waaruit ras of etnische afkomst blijkt, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, het lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid en gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. Het onrechtmatig gebruik van dergelijke bijzondere persoonsgegevens kan

namelijk een zeer grote impact hebben op de privacy. De verwerking van deze bijzondere categorieën persoonsgegevens is verboden, tenzij er een specifieke uitzondering van toepassing is, of de betrokkene uitdrukkelijk toestemming heeft gegeven voor de verwerking. Indien het niet nodig is om deze bijzondere gegevens te verwerken dan moet een organisatie dat ook niet doen.

Tip 4 Heb je het recht om persoonsgegevens te verwerken?

Je hebt alleen het recht om (gewone) persoonsgegevens te verwerken als je je kunt baseren op minimaal 1 van de 6 AVG-grondslagen. Eén van de grondslagen is dat **de betrokkene toestemming gegeven** heeft voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden. **Ook gerechtvaardigd belang** is een mogelijke grondslag. Organisaties moeten hierbij wel hun belangen om persoonsgegevens te verwerken om hun doelstellingen te bereiken afwegen tegen de rechten van het individu. De uitkomst van deze afwegingstest bepaalt of persoonlijke gegevens kunnen worden verwerkt zonder toestemming nodig te hebben.

De toestemming voor het verwerken moet onder de AVG expliciet gegeven zijn en aangetoond kunnen worden door de organisatie. Zorg daarom dat de toestemming en de datum waarop die gegeven is vast ligt. Let ook op dat expliciet inhoudt dat bijvoorbeeld het hokje om toestemming te geven zelf aangevinkt moet worden.

Tip 5 De ledenlijst beschikbaar voor eigen leden

Een vereniging mag in principe een ledenlijst beschikbaar stellen aan eigen leden. Wij raden wel aan om de ledenvergadering eenmalig te verzoeken om daarmee in algemene zin in te stemmen, mocht dit nog niet gebeurd zijn. De Autoriteit Persoonsgegevens is van oordeel dat het online publiceren van een ledenlijst slechts is toegestaan op een voor leden afgeschermde webpagina. Wil je als vereniging dus mogelijk maken dat leden elkaar kunnen zoeken via jouw app of website, zorg dan dat je die informatie uitsluitend aan eigen leden beschikbaar stelt.

Tip 6 Heb je toestemming nodig voor het maken en publiceren van beeldmateriaal?

Foto's en video's met een herkenbaar in beeld gebrachte betrokkene zijn meestal persoonsgegevens. Voor het maken en publiceren ervan heb je daarom meestal toestemming nodig van de betrokkene. Voor veel situaties kun je dit op voorhand oplossen door het opnemen van een algemene toestemmingsbepaling in de lidmaatschapsvoorwaarden of evenementvoorwaarden. Wil je toestemming van een persoon jonger dan 16 jaar? Dan vraag je de ouder/wettelijk vertegenwoordiger om toestemming.

Zorg ervoor dat leden en andere betrokkene op enige manier zijn geïnformeerd over eventuele beeldopnamen. Dat kan bijvoorbeeld in huisreglementen of met behulp van een bordje op de locatie.

Let op: iemand die toestemming geeft voor het maken van een foto, geeft daarmee niet per definitie toestemming voor de publicatie ervan. Een herkenbaar in beeld gebrachte persoon heeft in sommige gevallen het recht om zich te verzetten tegen publicatie van dergelijke beelden. In de regel zal je gehoor moeten geven aan een dergelijk verzoek.

Tip 7 Sponsoren en NAW- en e-mail gegevens van leden

Sponsoren hebben vaak interesse in NAW-gegevens van leden, zodat zij commerciële boodschappen kunnen versturen. Het doorgeven van NAW-gegevens is echter niet zomaar toegestaan, en vereist in principe uitdrukkelijke toestemming van een lid. Als het versturen van reclame per post door

sponsoren aan leden echter in algemene zin is goedgekeurd door de ledenvergadering, dan heb je voor de verstrekking van NAW-gegevens aan een sponsor geen individuele toestemming meer nodig.

Zorg wel dat je het voornemen tot doorgifte vooraf via de gebruikelijke wegen (nieuwsbrief, ledenblad) met leden communiceert, en geef leden gedurende een redelijke termijn de kans om zich te verzetten tegen de verstrekking van hun eigen NAW-gegevens aan sponsoren.

Voor de verstrekking van e-mailadressen geldt een strenger regime. Een sponsor mag vanwege de SPAM-regels namelijk geen commerciële berichten versturen zonder uitdrukkelijke toestemming van individuele ontvangers. Heeft de sponsor een dergelijke toestemming niet verkregen (al dan niet via jouw vereniging), dan heb je dus in principe geen legitieme reden om de e-mailadressen te verstrekken.

Stap 3 de rechten van de betrokkenen

Onder de Algemene verordening gegevensbescherming (AVG) krijgen betrokkenen meer mogelijkheden om voor zichzelf op te komen als hun persoonsgegevens worden verwerkt. Dit zijn de AVG-privacyrechten:

- Recht op inzage. Dat is het recht van mensen om de persoonsgegevens die je van hen verwerkt in te zien.
- Recht op rectificatie en aanvulling. Het recht om de persoonsgegevens die je verwerkt te wijzigen.
- Het recht op beperking van de verwerking: Het recht om minder gegevens te laten verwerken.
- Het recht met betrekking tot geautomatiseerde besluitvorming en profilering. Oftewel: het recht op een menselijke blik bij besluiten.
- Het recht om bezwaar te maken tegen de gegevensverwerking.
- Het recht op dataportabiliteit. Het recht om persoonsgegevens over te dragen (NIEUW).
- Het recht op vergetelheid. Het recht om ‘vergeten’ te worden (NIEUW).

Ten slotte hebben betrokkenen recht op duidelijke informatie over wat de organisatie met hun persoonsgegevens doet.

DOEN

Onderzoek of jouw organisatie kan voldoen aan de rechten van de betrokkenen en richt hiervoor interne processen in. Alle relevante medewerkers en vrijwilligers moeten zich bewust zijn van de rechten die de betrokkenen hebben en de wijze waarop je organisatie met verzoeken moet omgaan.

Informeer betrokkenen over de rechten die zij hebben en hoe zij daarvan gebruik kunnen maken. Deze informatie moet duidelijk, transparant en toegankelijk zijn.

Neem daarom de rechten van betrokkenen op in jullie Privacyverklaring, zodat het voldoet aan de AVG. Voordat een betrokkene toestemming geeft, moet hij/zij het Privacyverklaring hebben ontvangen of kunnen inzien en opslaan. Zodat je vanaf 25 mei 2018 op de juiste manier gehoor kunt geven aan verzoeken van mensen die hun rechten uitoefenen.

- Wijs mensen op de privacyrechten die zij hebben. Bijvoorbeeld via je privacyverklaring.
- Informeer mensen duidelijk over hóe zij een verzoek bij je kunnen indienen.

- Zorg dat het voor mensen makkelijk om een verzoek bij je te kunnen doen. Wanneer iemand elektronisch (bijvoorbeeld per e-mail) een verzoek doet, dan moet je de gevraagde informatie ook elektronisch geven.
- Reageer zo snel mogelijk maar in ieder geval binnen 1 maand op een verzoek. Concreet betekent dit dat je binnen die termijn ofwel het verzoek moet hebben uitgevoerd en de verzoeker hierover hebben geïnformeerd, of hebben aangegeven waarom je geen gehoor geeft aan het verzoek.

Stap 4 Vastleggen hoe de organisatie met de data omgaat

Organisaties hebben een verantwoordingsplicht in de nieuwe AVG. Dat betekent dat je vast moet leggen wie verantwoordelijk is voor de data, aan wie informatie wordt verstrekt en ook op welke computer deze wordt opgeslagen en op welke wijze deze wordt beschermt tegen virussen en hacken.

Niet onbelangrijk: verspreiding van data over verschillende computers of systemen zonder dat dat is vastgelegd kan uitgelegd worden als datalekken.

DOEN

Maak een overzicht van je verwerkingen. Documenteer welke persoonsgegevens je verwerkt en met welk doel je dit doet, waar deze gegevens vandaan komen en met wie je ze deelt.

Je kunt het verwerkingsregister ook nodig hebben als betrokkenen hun privacyrechten uitoefenen. Als zij vragen hun gegevens te corrigeren of verwijderen, moet je dit doorgeven aan de organisaties waarmee je hun gegevens hebt gedeeld. Beschrijf hoe je gegevens verwerkt. Doe dat zo overzichtelijk en duidelijk mogelijk. Liefst geen complexe procedures die niemand begrijpt of nog kan volgen. Kijk bijvoorbeeld bij tip 9 over wat je vast zou kunnen leggen over je dataverwerking.

Maak ook **procedures** over hoe je personen toegang geeft tot de informatie.

Met externe gebruikers van de bestanden, zoals drukkers, verspreiders van de nieuwsbrieven en bijvoorbeeld de koepelorganisatie, moet je overeenkomsten opstellen voor het gebruik van gegevens; de zogenoemde **verwerkersovereenkomst**. In deze overeenkomsten moeten bijvoorbeeld ook afspraken gemaakt worden over het vernietigen van de gegevens na gebruik. Ook wanneer het om de koepelorganisatie gaat, moet je afspraken maken over het gebruik van de bestanden. De organisaties maken immers afspraken met de leden over het zorgvuldig bewaren van hun gegevens en daar kan een organisatie op aangesproken worden.

Tip 8

Hoe je je gegevens beveiligd is niet expliciet voorgeschreven. Denk bij beveiliging aan goede beveiligingssoftware op de pc's, eventueel passwords op de excel en word documenten mocht je die gebruiken voor de vastlegging van de gegevens. Maak ook gebruik van afgesloten delen van de website met toegangscodes voor bijvoorbeeld je ledenlijst en aanmelden voor activiteiten.

Tip 9

De AVG stelt een verwerkingsregister verplicht voor organisaties met meer dan 250 personen in dienst. Een organisatie met minder dan 250 personen in dienst hoeft alleen een register bij te houden bij risicovolle verwerkingen (zoals het opstellen van klantprofielen, of het verwerken van

grote hoeveelheden gegevens), **wanneer structureel persoonsgegevens verwerkt worden**, of bij het verwerken van gevoelige gegevens.

Je verwerkt al gauw structureel persoonsgegevens als het gaat over je ledenadministratie. Dus leg een verwerkingsregister aan.

Wat staat er in het register?

- de naam en contactgegevens van verantwoordelijke (of diens vertegenwoordiger, wanneer de verantwoordelijke buiten de EU is gevestigd), en van de functionaris voor gegevensbescherming (indien aanwezig);
- de doeleinden waarvoor gegevens worden verwerkt;
- de categorieën gegevens (zoals NAW-gegevens, contactgegevens, betaalgegevens);
- de categorieën betrokkenen (bijvoorbeeld: klanten, websitebezoekers, werknemers);
- de categorieën ontvangers (aan wie worden de gegevens verstrekt?);
- informatie over eventuele doorgifte van gegevens naar landen buiten de EU;
- de bewaartermijnen van de gegevens;
- de manieren waarop gegevens zijn beveiligd (bijvoorbeeld: virus-scanners op de PC's en laptops, encryptie, logische toegangscontrole).

Tip 10
Denk ook aan het beveiligen van je website. Een SSL-certificaat verhoogt de veiligheid van een website door de gegevens te versleutelen. Op deze manier kunnen de gegevens niet worden gelezen door cybercriminelen die proberen om data te onderscheppen. Dit is met name belangrijk voor websites waar de gebruikers kunnen inloggen met een wachtwoord, of voor webshops. Een SSL-certificaat kun je regelen via je webhosting aanbieder.

Stap 5 Procedure opstellen voor het melden van datalekken

Elke organisatie die persoonsgegevens opslaat, is verplicht datalekken te melden binnen 72 uur na ontdekking. Om dit zorgvuldig te doen is het handig vooraf procedures af te spreken.

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. In de meeste gevallen gaat het om uitgelekte computerbestanden, een gestolen geprinte ledenlijst of cliëntgegevens. Andere voorbeelden zijn cyberaanvallen, verkeerd verzonden e-mail, gestolen laptops, afgedankte niet-schoongemaakte computers en verloren usb-sticks.

Tenzij het datalek waarschijnlijk geen nadelige gevolgen heeft voor de betrokken personen, moet het lek tijdig worden gemeld bij de Autoriteit Persoonsgegevens. Heeft het lek bovendien een hoog risico op nadelige gevolgen voor de personen wiens gegevens het betreft, dan moet het incident ook aan deze personen worden gemeld.

DOEN

Zorg dat iedereen zich bewust is dat er zorgvuldig omgegaan moet worden met persoonsgegevens. Zorg voor goede beveiliging.

Maak een procedure voor de onverhoopte situatie dat er een datalek is. In de procedure staat:

- Bij wie in de organisatie een datalek gemeld moet worden;
- Wie binnen de organisatie nog meer geïnformeerd moet worden;
- Wie checkt wat er gelekt is;
- Hoe in kaart gebracht wordt wat de gevolgen zijn voor de personen van wie de persoonsgegevens gelekt zijn;
- Welke gegevens nodig zijn voor de melding. 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 de organisatie heeft genomen of voorstelt te nemen om deze gevolgen te verhelpen.
- Wie de melding doet bij de Autoriteit Persoonsgegevens.

Meldingen kunnen digitaal gedaan worden bij het meldloket van de Autoriteit Persoonsgegevens: http://datalekken.autoriteitpersoonsgegevens.nl

Overzicht van de belangrijke documenten:

- Privacyverklaring
- Register verwerkingsactiviteiten
- Procedure voor het omgaan met persoonsgegevens
- Toestemmingverklaring voor persoonsgegevens (en gebruik foto's en filmmateriaal)
- Verwerkersovereenkomst
- Procedure datalek