Voldoen aan de AVG voor verenigingen en stichtingen

Heinrich W. Klöpping, MSc CISSP CCSP CIPP/E SCI

Over de Algemene Verordening Gegevensbescherming – de AVG - wordt veel geschreven de laatste tijd. Deze nieuwe Europese wet kan vanaf 25 mei 2018 worden gehandhaafd. Dat doet de Autoriteit Persoonsgegevens (AP). Die kunt u zien als de "politie" van de AVG. Net als de politie heeft ook de AP de bevoegdheid boetes uit te delen. Die boetes kunnen heel hoog zijn. Hoewel de kans dat de Autoriteit Persoonsgegevens in mei bij u op de stoep staat klein is[1], is het toch goed om er nu werk van te maken. Het biedt een mooie kans om op te ruimen en uw organisatie weer eens "mooi strak in de lak te zetten"! En u helpt de wereld een stukje veiliger te maken. Doen dus!

Tegenwoordig stromen gegevens heel makkelijk over de hele wereld. Op het Internet maakt men dankzij vrij verkeer van informatie profielen van mensen. Daaruit blijkt wat iemands interesses zijn, bijvoorbeeld aan de hand van bezoek aan websites. Enerzijds mooi, want mensen krijgen dan alleen zaken aangeboden waar ze interesse in hebben. Anderzijds kunnen kwaadwillenden de gegevens misbruiken. Bijvoorbeeld iemand lastig vallen die een overtuiging of geaardheid heeft die hen niet zint. Men kan die gegevens ook gebruiken om zich onder andermans identiteit voor te doen, bijvoorbeeld om aankopen te doen van dubieuze zaken onder andermans naam. Maar niet alleen op het Internet worden gevoelige gegevens verwerkt: ook binnen uw stichting of vereniging heeft u vaak dergelijke gegevens in beheer. Uw ledenadministratie bijvoorbeeld. Die gegevens zijn voor kwaadwillenden ook interessant. De privacy is in het geding.

Het recht op privacy is een Europees grondrecht, dat we in toenemende mate beschermen met steeds krachtiger maatregelen en wetten. De AVG is een recent voorbeeld van zo'n wet. De wet geldt in alle 28 landen van de EU en gaat over het verwerken van gegevens van natuurlijke personen (mensen). Als u gegevens verwerkt van mensen die verblijven in de EU is de wet van toepassing. Dus ook buiten Europa[2].

De wet is al in april 2016 aangenomen maar men heeft organisaties 2 jaar de tijd gegeven hun zaken op orde te krijgen. Die termijn loopt af op 25 mei 2018. U had dus formeel al voor die tijd alles moeten hebben geregeld om aan de wet te voldoen.

Als u bestuurder of anderszins betrokkene bij een stichting of vereniging bent en dit document leest is de kans groot dat u nog niets heeft gedaan. U vraagt zich af wat u nu moet doen. Een volledig sluitend recept is niet te geven. Wel is er een richtlijn te geven hoe te handelen. Dit document geeft deze hoofdlijn en ook een algemeen plan van aanpak om te kunnen voldoen aan de AVG.

Elke stichting of vereniging is uniek. Dit document geeft een richting, maar u doet er goed aan om tijdig een deskundige te raadplegen. Volledigheidshalve: aan dit document kunt u geen rechten ontlenen, het is een goedbedoeld gratis advies.

1 De AP is een kleine organisatie met beperkte middelen en heeft van de 2e kamer ook nog eens bij motie de missie gekregen de wet niet al te streng te handhaven.

2 Omdat de EU buiten haar eigen territorium geen recht kan opleggen wordt dat geregeld door middel van het afsluiten van contracten en internationale overeenkomsten.

De hoofdlijn

Om 'persoonlijke' data te kunnen beschermen moet u eerst weten wat 'persoonlijke data' is. Dan bepaalt u of en waar u persoonlijke data verwerkt. Daarna bepaalt u of u meer of minder persoonlijke data wilt verwerken. De richtlijn is: zo weinig mogelijk maar zoveel als nodig is. Het verschilt daarbij of u de gegevens in opdracht verwerkt of dat u zelf bepaalt wat u verwerkt. U werkt aan bewustwording, opleiding en u documenteert. U maakt een deel van die documenten openbaar. Verder moet u waarschijnlijk een aantal nieuwe processen of procedures introduceren, bijvoorbeeld een proces dat beschrijft wat u moet doen als iemand van u wil weten welke persoonlijke gegevens u van hem of haar heeft. Dit document geeft een voorbeeld van een aanpak: het introduceren van een programma voor introductie van de AVG in uw stichting of vereniging. Dat programma voor introductie is eindig, maar de inspanning houdt nooit op zo lang de AVG er is.

Wat is persoonlijke data

Strikt genomen is persoonlijke data die data die naar één persoon of een zeer beperkt aantal personen verwijst. Een eenvoudige vuistregel is: als u er “mijn” voor kunt zetten is het persoonlijke data. Bijvoorbeeld: mijn voornaam, of mijn IP adres. Bij verenigingen en stichtingen gaat het vaak om voor- en achternaam, geboortedatum, geboorteplaats, adresgegevens, telefoonnummer, e-mailadres, geslacht, IP-adres, locatiegegevens, welke websites iemand bezoekt, contactenlijst uit een app, welke browser gebruikt wordt op welk apparaat, bankrekeningnummer.

Als u twijfelt of iets persoonlijke data is, gaat u er dan vooralsnog van uit dat dat het geval is. Beter iets te veel goed beschermd dan iets te weinig.

Wanneer mag u persoonlijke data verwerken

Er moet een reden voor u zijn om persoonlijke data te verwerken. De AVG noemt in artikel 6 de zes grondslagen om persoonlijke data te mogen verwerken.

1. Toestemming: u heeft (aantoonbaar) toestemming van de persoon gekregen voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden. Merk op dat iemand die toestemming heeft gegeven ook expliciet het recht heeft die toestemming op elk gewenst moment weer in te trekken.
2. Overeenkomst: De verwerking is noodzakelijk voor de uitvoering van een overeenkomst met de persoon.
3. Wettelijke verplichting: naast de AVG zijn er meer wetten in Nederland en de EU. Soms moet u persoonsgegevens verwerken om te voldoen aan een wettelijke verplichting, bijvoorbeeld als werkgever een kopie hebben van het paspoort van uw werknemer.
4. Vitaal belang: De verwerking is noodzakelijk om de vitale belangen van de persoon of een ander natuurlijke persoon te beschermen. Denkt u aan het raadplegen van persoonsgegevens om een leven te kunnen redden.

5. Publiekrechtelijke taak: bij de vervulling van een taak van algemeen belang of uitoefening van het openbaar gezag. In dat geval heeft u een opdracht van de overheid om de gegevens namens haar te verwerken.
6. Gerechtvaardigd belang: ook u heeft belangen en rechten. Als u daartoe echt de gegevens van iemand moet verwerken mag dat, behalve wanneer de belangen van de betrokkene anders eisen. Dat laatste met name wanneer de betrokkene een kind is. Een voorbeeld is als iemand nog schulden bij uw organisatie heeft: u hoeft zijn of haar gegevens niet te wissen als hij of zij daar om vraagt omdat u anders uw gerechtvaardigd belang niet uit kunt oefenen.

Werkt u in opdracht of bepaalt u zelf

U kunt de persoonsgegevens moeten verwerken voor een andere organisatie, of voor uw eigen organisatie. In het laatste geval bepaalt u hoe u met de persoonsgegevens om wilt gaan, in het eerste geval wordt u aangestuurd door een andere organisatie. Merk op dat u in beide gevallen verantwoordelijk bent voor de correcte verwerking van de gegevens en dat degenen van wie de gegevens zijn u hier op aan kan spreken. Het is dan aan u om eventuele vergoeding van schade of opgelegde boetes bij de andere partij(en) te verhalen.

Documenten

Een aantal documenten is verplicht door de wetgever. Dit zijn het verwerkingsregister, de DPIA (als nodig), een beschrijving van uw privacy beleid in eenvoudige woorden, een document dat beschrijft hoe lang u data bewaard, eventueel een formulier waarmee mensen toestemming voor de verwerking kunnen geven en overeenkomsten met leveranciers voor verwerking van gegevens.

Nieuwe processen / procedures

Organisaties moeten, bijvoorbeeld, beleid hebben om te kunnen bepalen wanneer bepaalde data niet langer bewaard hoeft te worden; hoe personen in staat worden gesteld toestemming in te trekken en hoe om te gaan met verzoeken van gebruikers die bezwaar maken tegen verwerking van hun gegevens.

Welke autoriteit

U heeft normaal gesproken te maken met één autoriteit. In Nederland is dat de Autoriteit Persoonsgegevens. Heeft uw organisatie vestigingen in meerdere EU-lidstaten? Of hebben uw gegevensverwerkingen in meerdere lidstaten impact? Dan hoeft u onder de AVG nog maar met één privacytoezichthouder zaken te doen. In het algemeen is deze zogenaamde “leidende toezichthouder” de toezichthouder van het land waar uw hoofdvestiging zich bevindt.

FG (DPO)

De Functionaris Gegevensbescherming is een bijzondere rol, die in principe alleen hoeft te worden ingevuld als er hoog risico bestaat op inbreuken in de privacy. De wet stelt een aantal eisen aan FG's. Het moet een natuurlijk persoon zijn. De FG moet voldoende kennis hebben van de privacywetgeving en de organisatie. Hij moet betrouwbaar zijn wat zich onder meer uit in een geheimhoudingsplicht.

De FG geniet, wanneer hij in dienst is van een organisatie, speciale bescherming. Hij kan niet worden ontslagen omdat hij zijn functie uitoefent. Daaronder valt dat de organisatie wettelijk verplicht is om de FG controlebevoegdheden te geven: hij mag alle ruimtes betreden, zaken onderzoeken en inlichtingen en inzage vragen. De FG moet in onafhankelijkheid zijn werkzaamheden kunnen verrichten binnen de organisatie. Hij of zij kan geen sancties opleggen, maar kan bijvoorbeeld wel rechtstreeks met de AP contact opnemen.

Uw HHR

Een vereniging of stichting kan een huishoudelijk reglement hebben. Het is goed daarin een bepaling op te nemen waarin u aangeeft dat informatiebeveiliging voor u een belangrijke zaak is. Strikt genomen hoeft het niet waar het gaat om de AVG, dat is immers een wet en die geldt hoe dan ook. Maar net als u in een HHR ook kunt opnemen dat bestuurders er alles aan zullen doen om ruzie te voorkomen en zo de toon voor het besturen te zetten, is dit ook mogelijk voor informatiebeveiliging.

Een voorbeeld van een dergelijk clausule is:

> "*Het bestuur geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt. Zij doet dit onder meer door het publiceren en handhaven van een informatiebeveiligingsbeleid. Het beleid is van toepassing op de gehele organisatie, alle medewerkers, alle processen, alle organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid van de Stichting is in lijn met het algemene beleid van het bestuur en de relevante landelijke en Europese wet- en regelgeving.*"

Eventueel kan hier nog aan toe worden gevoegd:

> "*Het Bestuur baseert haar beveiligingsbeleid op wat is gesteld in de Code voor Informatiebeveiliging (NEN/ISO 27002:2007) en gebruikt de "Tactische baseline informatiebeveiliging Nederlandse Gemeenten (BIG)" als uitgangspunt voor haar baseline.*"

Een plan van aanpak

In de figuur hiernaast (met dank aan TRUSTe) ziet u een mogelijke weg door het proces om een goede nakoming van de AVG in een bedrijf te kunnen realiseren. Dat pad is niet veel anders voor uw stichting of vereniging, al zal het vaak om kleinere groepen mensen en minder gevoelige data gaan. Ook zijn in een vereniging of stichting de lijnen vaak wat korter en de sfeer wat informeler. De stappen zijn:

De nulfase: die staat niet in het plaatje hierboven. Het is de fase waar u nu waarschijnlijk in bent: u weet dat u iets moet doen, maar geen idee wat en met wie en hoe. Dus leest u bijvoorbeeld dit document. Omdat u dit leest heeft u waarschijnlijk betrokkenheid bij de stichting of vereniging en een ingang bij het bestuur. Uw rol zou kunnen zijn het bestuur te bewegen om actie te ondernemen. U kunt bijvoorbeeld een samenvatting van dit document presenteren, of een ter zake kundige vragen om dat te doen.

De kernvraag in de nulfase is vaak: "moeten we hier iets mee, waarom zouden we dit doen?". Het antwoord is heel eenvoudig: ja, u "moet" hier iets mee, het is een wet en die geldt voor ieder in Europa (en daarbuiten) die persoonsgegevens van mensen in Europa verwerkt. Maar het geeft u ook voordelen: door de juiste maatregelen te nemen om aan de wet te voldoen biedt u de mensen waar u mee werkt en voor werkt zekerheid dat er netjes met hun gegevens wordt omgegaan. U krijgt er ook een goed inzicht mee wat er in uw vereniging of stichting aan informatie omgaat en kunt zo passende maatregelen treffen om dat veilig en verantwoord te doen. En het kan zelfs zo zijn dat u door de analyse van wat u doet nieuwe kansen gaat zien voor het uitvoeren van uw werk.

Programma en team opstellen, dat begint met de vraag: *wie zijn betrokken.* In vaktaal ook wel: 'wat is de scope'. Als het gaat om een kleine stichting of vereniging dan is vaak iedereen betrokken. Bij grotere organisaties is het beter eerst een onderdeel van de organisatie als startpunt te gebruiken. Als het daar goed lukt om de AVG in te bedden dan is er een werkend voorbeeld en is ook bekend welke problemen er waren en hoe die op te lossen zijn. Ook zijn de mensen die aan het project meewerkten vaak enthousiast over hun succes, wat motiverend werkt op de rest van de organisatie. En tenslotte krijg je zo een beter beeld van de inspanningen en kosten.

Waar vinden we mensen, geld en middelen? Als het bestuur overtuigt is van de noodzaak om in actie te komen en het bereik heeft bepaald zal het ook middelen ter beschikking moeten stellen.

Die zijn in eerste instantie nodig om een programma op te stellen. Zo'n programma bestaat uit een aantal projecten, die soms overlappend of naast elkaar worden uitgevoerd, zie het plaatje hier boven. Soms worden bepaalde projecten niet gedaan omdat het niet nodig is in uw organisatie, bijvoorbeeld certificatie.

Een complicerende factor is dat er in het algemeen nog niet veel kennis aanwezig is over wat je moet doen om de AVG goed in te bedden. En het bestuur weet vaak ook niet waar men staat en nog maar heel globaal waar men naar toe wil - dus is de weg niet helder. Daardoor zijn de te verwachten inspanningen / kosten in deze fase alleen grof te bepalen.

Er zijn binnen het programma een aantal rollen te onderscheiden: de sponsor, de kampioen, de expert, de programmamanager en eventueel een FG.

- De sponsor is de partij met het geld en de middelen. Dat is in de praktijk bij een vereniging of stichting dus het bestuur.
- Het bestuur kan beginnen met het aanwijzen van een kampioen. Dit is vaak iemand van het bestuur met interesse in de zaak, die de kar trekt, voorlichting geeft en aanspreekpunt is. Let op dat de persoon die wordt benoemt de juiste kennis en kunde heeft - of daar snel aan kan komen.
- Bijvoorbeeld kan zo'n kampioen een jurist of privacy expert raadplegen. Dat kost geld: gemiddeld betaalt men voor een expert al gauw 130-180 euro per uur, tarieven die men bij advocatenkantoren hanteert zijn vaak het dubbele. De "gekte" rond de AVG leidt ook wel eens tot gelegenheidsexperts. U kunt helaas niet aan hun neuspunt zien of ze er verstand van hebben, maar u kunt wel letten op hun accreditaties. Voorbeelden van bona fide accreditaties zijn die van de IAPP (CIPP/E, CIPM, CIPT, FIP) en de NOREA accreditatie (RE).
- Het programma draait altijd onder verantwoordelijkheid van het bestuur, maar soms wijst men expliciet een programmamanager aan. Eventueel kan het bestuur het uitvoerend programmamanagement delegeren aan een commissie of aan de kampioen maar het moet een actieve rol blijven spelen in het proces. De expert brengt advies uit en dient dat onbezwaard te kunnen doen, het is dus *niet* handig hem of haar de programmamanager te maken
- *Is een FG nodig:* speciale aandacht is nodig voor de vraag of het nodig is een Functionaris Gegevensverwerking aan te stellen. Als u maar weinig persoonlijke data beheert en/of verwerkt is het antwoord vrijwel altijd "nee". Als het wél nodig is een FG te benoemen kan het een optie zijn deze FG deeltijds in te huren. Vaak kent de expert die u raadpleegt de mogelijkheden wel. Pas wel op dat een FG een onafhankelijke rol speelt en dat het daarom niet mag dat een bestuurder deze rol invult. Die komt daarmee mogelijk in conflict met zichzelf: als bestuurder zou hij misschien wel anders adviseren dan de FG *moet* doen..

Wat is de missie en zijn de doelen? De kampioen bepaalt samen met het bestuur en de expert wie bij het programma betrokken zijn, wat de missie is, welke doelen men wil bereiken, hoe men meet dat die bereikt zijn en men maakt een gedetailleerdere kostenschatting en planning. Het bestuur dient vervolgens in redelijkheid te borgen dat deze kosten gedragen kunnen worden en het met de planning eens te kunnen zijn. Zonodig na bijstelling en accordering door bestuur, expert en eventueel (beoogd) FG gaan de volgende fasen in.

Er worden dan projecten opgestart. Als u niet zo goed weet wat 'een project' is: dat is niet anders dan een serie activiteiten, die u met een aantal mensen binnen een bepaalde tijd uitvoert met een meetbaar resultaat.

Bewust maken en risico's in kaart brengen: Het eerste project is vaak dat van bewustmaking. Dat kan enige weken tot enige maanden duren. U richt zich op alle betrokkenen. In vaktaal: op allen die 'in scope' zijn.

De kampioen, ondersteund door de expert, richt zich eerst op de bestuurders. Dat is in de nulfase begonnen en gaat nu door. Tijdens deze fase word vaak begonnen met het verzamelen van informatie over de gegevens die in de organisatie worden beheerd. Van belang is dat management (bestuur) het initiatief volledig steunt en er ook daadwerkelijk middelen voor vrij wil maken.

Hoe snel u iedereen op de hoogte heeft hangt af van de frequentie waarmee u met de mensen in aanraking komt en de prioriteit die er aan wordt gesteld. Dit 'awareness' of bewustwordingsproject is van groot belang voor het slagen van de rest van het programma, zeker in een vrijwilligersorganisatie waar het middel 'geld' meestal niet gebruikt kan worden om mensen te motiveren aan het werk te gaan.

Inventariseer gegevens en hun gebruik. U bepaalt vervolgens welke persoonsgebonden data u al verwerkt in uw organisatie. Het in kaart brengen van de persoonlijke data doet u in een document of spreadsheet. Dit is een aanzet tot het zogenaamde 'register van verwerking'. Daarin staat welke data u heeft en wat u er mee doet. Dit document moet u kunnen overleggen aan de AP als die er om vragen.

Maak een risico- en verschilanalyse. Als u weet wat u verwerkt en waarom kunt u bepalen of dat nodig is, of eventueel meer of mogelijk minder nodig is. Het kan zijn dat u al jaren persoonsgegevens in uw bezit heeft waar u eigenlijk niets meer mee doet. Bijvoorbeeld van ex-leden. Maar ook van de mensen waar u nu mee en voor werkt zou het kunnen dat u te veel data van hen heeft. Denk bijvoorbeeld aan adres en woonplaats, of geboortedatum. Doet u er nooit iets mee, of zou u er best zonder kunnen? Dan is het beter die data niet in uw bezit te hebben.

Als voorbeeld: het zou kunnen dat u al jarenlang gebruik maakt van een registratieformulier waarop mensen ook hun bankrekeningnummer in moeten vullen. Maar dat nummer gebruikt u alleen maar als mensen van u een vergoeding krijgen. En lang niet iedereen krijgt zo'n vergoeding. U heeft zo informatie waar u niets aan heeft maar die u wél zorgvuldig moet beschermen. Misschien is het wel veel beter die informatie NIET standaard te vragen, maar alleen als iemand geld van u krijgt.

U moet er in deze fase over nadenken wat de consequenties van het in bezit hebben van deze data zijn. Maar u kunt in deze fase ook bedenken dat u misschien wel ***meer*** persoonsgegevens zou willen hebben – en waarvoor. Misschien wilt u wel beginnen met het gedrag van mensen vastleggen die uw website bezoeken en op hen een gerichte wervingscampagne opstarten.

De situatie die u uiteindelijk wilt verschilt vrijwel zeker van de huidige situatie. U bepaalt welke verschillen er zijn en hoe u van de huidige naar de gewenste situatie komt.

Ontwikkel beleid, processen en procedures. Organisaties moeten, bijvoorbeeld, beleid hebben om te kunnen bepalen wanneer bepaalde data niet langer bewaard hoeft te worden; hoe personen in staat worden gesteld toestemming in te trekken en hoe om te gaan met verzoeken van gebruikers die bezwaar maken tegen verwerking van hun

gegevens. Het verwijderen van dergelijke gegevens zal soms een hele uitdaging zijn. Denk aan het wissen van gegevens uit backups, of van alle PC's van alle bestuursleden. Denk aan mail die extern is opgeslagen bijvoorbeeld in een GMail account. Of aan de printjes die zijn gemaakt en die bij de penningmeester in een archiefkast zitten. En hoe gaat u de mailadressen wissen op de PC's van mensen waar u geen sturing over heeft? Denk aan het beruchte voorbeeld van per ongeluk versturen van mail aan grote groepen mensen waarbij alle mail adressen in een CC veld genoemd staan. U snapt dat het beter is om dit lekken van persoonsgegevens vooral te voorkomen, naderhand repareren is moeilijk.

Bij een verzoek tot vergetelheid moet op alle plaatsen waar de relevante gegevens van de persoon zich bevinden deze gegevens worden gewist. Dit betekent dus ook in backups, in papieren dossiers etc.

Besteed in deze fase ook aandacht aan de rechten van de mensen waarvan u de persoonsgegevens heeft en bedenk processen / procedures die deze rechten faciliteren:

1. Het recht op toegang
2. Het recht op correctie
3. Het recht op wissen (het 'recht om te worden vergeten')
4. Het recht om verwerking te beperken
5. Het recht op het overdragen van gegevens ('portability')
6. Het recht om bezwaar te maken
7. Rechten met betrekking tot geautomatiseerde besluitvorming en profilering.

Hanteer de regel: "bij twijfel over de noodzaak moet ik geen persoonsgegevens willen verwerken", net als de regel "bij twijfel of iets een persoonsgegeven is – dan is het dat."

Processen die te maken hebben met privacy by design en privacy by default komen in deze fase mogelijk ook aan bod. De term slaat op uw plicht om zo weinig mogelijk data te verzamelen ("privacy by default") en op uw plicht om in uw werk altijd rekening te houden met privacy ("privacy by design"). De geest zal duidelijk zijn. Uw expert kan u hierover voorlichten.

Manage de verwachtingen en leid op. Hoewel u in de eerdere fase al hebt gezorgd voor bewustwording wil dat niet zeggen dat de mensen die met persoonsgegevens gaan werken in uw stichting of vereniging plots zo maar weten wat ze moeten doen. Soms is ook specifieke kennis nodig rond wet- en regelgeving. U kunt besluiten een externe trainer in te huren, mensen op cursus te sturen, eventueel examen te laten doen (mogelijk inclusief accreditatie / certificatie, e.g. CIPT) of zelf cursussen te organiseren. Vergeet niet dat dat laatste wel vereist dat de juiste kwaliteiten aanwezig zijn. U kunt vaak uw kampioen en uw expert hierin een rol laten spelen. Wees bescheiden in wat u vraagt van uw mensen zodat men dat wat u vraagt strikt wil en kan naleven. Realisme en kleine stappen leidt vaak tot het beste resultaat.

Bepalen en implementeren maatregelen

Informeren en toestemming vragen – in de AVG kennen we 6 grondslagen voor verwerking. Slechts één daarvan is 'Er is toestemming gegeven'. Desondanks bent u

verplicht om de mensen waar u persoonsgegevens van heeft informatie te geven over hoe u met hun gegevens omgaat. Dat moet in heldere, klare taal. Het is goed om een zogenaamde 'privacyverklaring'[3] op uw website te publiceren[4]. Daarin beschrijft u in algemene zin en in eenvoudige, begrijpelijke taal, welke soorten privacy gevoelige informatie u heeft, wat u er mee doet, waarom, en met wie u die deelt. Mogelijk moet of wilt u wel een stap verder gaan en mensen rechtstreeks op de hoogte brengen. Dat is in ieder geval verplicht als u géén privacyverklaring online heeft. U kunt ze bijvoorbeeld per brief, per mail, persoonlijk etc. informeren. Als u wel een privacyverklaring heeft kunt u in uw communicaties verwijzen naar uw privacyverklaring. Het is goed de personen waar het om gaat ook uit te leggen welke rechten ze hebben en hoe zij van hun rechten gebruik kunnen maken - zoals het recht om vergeten te worden. U moet de Autoriteit Persoonsgegevens onder meer kunnen laten zien dat u mensen goed heeft geïnformeerd over de verwerking van hun persoonsgegevens. Het hebben van een online privacyverklaring wordt daarbij gezien als voldoende.

Im- en export van data en derden beheer – als uw vereniging of stichting zaken doet met derden en deze beschikken over persoonsgegevens die u hen aanlevert bent u verplicht met hen een overeenkomst af te sluiten om de regels waar u beiden aan moet voldoen vast te leggen. Verder kan een persoon wiens gegevens u heeft u vragen om hem of haar een overzicht te sturen van alle gegevens die van hem heeft. De AP publiceert voorbeeldbrieven die u eens zou kunnen inzien om te kijken hoe zo'n verzoek er uitziet. Ook kan iemand vragen deze gegevens in een gangbaar formaat (CSV, XML etc.) over te dragen aan een derde. U dient hiervoor processen en procedures te hebben.

De individuele rechten bepalen – in de stichting of vereniging zijn er verschillen in wie wat mag en moet kunnen zien en verwerken. Het is goed dit nauwkeurig te beschrijven en een register bij te houden wie waar op welk moment bij mag en waarom.

Fysieke, technische en administratieve beveiliging – mensen mogen niet bij gegevens kunnen waar ze niets mee te maken hebben. Maar de gegevens moeten wel vlot beschikbaar zijn voor degenen die ze moeten verwerken. In artikel 32 van de AVG worden een aantal maatregelen opgesomd: versleutelen of anonimiseren van gegevens; audits en het vermogen om bij een incident de toegang tijdig te herstellen. In deze fase bepaalt u welke maatregelen u wilt treffen. Ook moet u processen inregelen om de beschikbaarheid, vertrouwelijkheid, integriteit en veerkracht van de gegevens en diensten te borgen.

Maatregelen in de praktijk brengen en onderhouden

Risico analyse (DPIA) – wanneer een hoog risico bestaat voor de rechten en vrijheden van mensen wiens gegevens u verwerkt moet u volgens artikel 35 van de AVG een beoordeling van die risico's maken. Of dat hoge risico bestaat bepaalt u zelf[5]. Het is in ieder geval zo als u systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profiling. Ook als u op grote schaal bijzondere persoonsgegevens verwerkt of als u op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied

3 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/rechten-van-betrokkenen#hoe-stelt-u-een-privacyverklaring-op-6255

4 Denk daarbij ook aan het zonodig installeren van een SSL certificaat, zodat data tussen u en de gebruiker is beschermd en de gebruiker zekerheid heeft dat hij inderdaad met uw website te maken heeft.

5 Of u dat voldoende goed heeft gedaan zal de AP beoordelen mocht het daar van komen. U kunt zich dus niet vrijwaren door simpelweg te verklaren dat het niet nodig is in uw ogen.

(bijvoorbeeld met cameratoezicht). Deze *gegevensbeschermingseffectbeoordeling* wordt in de praktijk in Nederland ook vaak aangeduid als de DPIA, naar het Engelse "Data Protection Impact Assessment". De DPIA moet vóór aanvang van de verwerking worden gemaakt. Een stichting of vereniging die persoonlijke gegevens verwerkt met een dergelijk hoog risico is ook verplicht een FG te hebben, die hierin het voortouw neemt. De beoordeling bevat ten minste een beschrijving van de beoogde verwerkingen en doelen daarvan, een beoordeling of de verwerking redelijkerwijs nodig is om de doelen te bereiken en een beoordeling van de risico's voor de mensen waar het om gaat. Het is aan te raden om, ook als u denkt dat u geen hoog risico hebt, toch een DPIA te maken. NOREA, de beroepsorganisatie van IT-auditors in Nederland, heeft een handleiding voor het maken van een dergelijke risicoanalyse gepubliceerd op haar website[6]

Beleid rond bewaren en weggooien – in deze fase schrijft u op hoe lang u persoonsgegevens moet bewaren en wat u gaat doen om ze te verwijderen. U houdt daarbij rekening met uw wettelijke en contractuele verplichtingen, u kunt bijvoorbeeld iemands gegevens soms niet mogen wissen omdat u bij overeenkomst nog zaken moet afhandelen waarbij u die gegevens nodig heeft. De algemene regel is weer: "bewaar niets dat u niet nodig hebt".

Volledigheid en kwaliteit van gegevens – in deze fase schrijft u op hoe u zorgt dat de gegevens actueel blijven en hoe u hun integriteit borgt. U kunt bijvoorbeeld de mensen waar u gegevens van heeft een mogelijkheid geven die (beschermd) te raadplegen en daar correcties op door te geven. Wees voorzichtig met het mailen van persoonsgegevens, omdat deze in principe onbeschermd over het Internet reizen. Een mogelijkheid is om mensen te vragen in te loggen en ze zo hun gegevens te tonen. Of u gebruikt een medium dat beschermd is, bijvoorbeeld versleutelde mail of een papieren brief.

Proces bij een inbreuk – en dan gaat het toch mis. In de consternatie is het goed (en ook verplicht) om een helder proces te hebben dat u kunt volgen als er toch onverhoopt persoonsgegevens zijn uitgelekt. U moet dat in principe binnen 72 uur aan de AP melden. Daarbij is het niet langer van geen belang of het weinig of veel data betrof. Wel is van belang hoe groot de kans is dat het lek voor de betrokkene gevolgen heeft.

Laat steeds uw toewijding zien. De AVG implementeren is een traject, geen project. Het houdt nooit op en u moet dus constant alert zijn op de persoonsgegevens en hun vewerking. Omdat er snel een vorm van bedrijfsblindheid kan optreden is het goed om geregeld een externe auditor te vragen naar uw situatie te kijken. Verder zult u als bestuur verslag willen hebben van de gang van zaken voor wat betreft het verwerken van persoonsgegevens, bijvoorbeeld: hoeveel verzoeken tot inzage er zijn geweest, of deze vlot en naar tevredenheid konden worden afgehandeld en zo voort. Verder is het zaak om alle betrokkenen te blijven scholen en hun bewustzijn van de AVG en de daaruit voortkomende verplichtingen voldoende groot te houden. Dat kan op allerhande manieren: een forum, een website, mail aan betrokkenen, interne cursus, on-line cursus, reclamematerialen (stickers, posters, koffiemokken), aan de orde brengen bij commissievergaderingen of in (functionerings)gesprekken met betrokkenen en zo voort. Besteed er ook op uw openbare website aandacht aan.

---

6 https://www.norea.nl/download/?id=522

Bepaal hoe goed de audits werken – het houden van audits is niet voldoende. Wat doet uw vereniging of stichting met de uitkomsten? Is er sprake van verbetering? Zo niet, wat kunt u daar aan doen? De processen om dit te bepalen worden in deze fase opgesteld.

Interne- en externe verslaglegging – wat u als bestuur wilt weten bepaalt u grotendeels van te voren. Dat schrijft u op, en ook hoe u zich voorstelt aan die informatie te komen. Dan is het zaak om de verslagleggingen met regelmaat in een bij voorkeur gestandaardiseerd formaat aangeleverd te krijgen. Dit mag vooral geen "procedure om de procedure" worden, of een klakkeloos invullen van een checklistje, het is zaak dat de opstellers zich daadwerkelijk interesseren in de materie, dus ook: goed opgeleid / voorgelicht en gemotiveerd. Dat is nog van veel groter belang als u toch nog ad hoc informatie behoeft.

Privacy notitie en hoe je disputen oplost – de privacyverklaring is eerder al aan de orde geweest. Een algemene beschrijving van hoe uw organisatie met privacy omgaat, welke gegevens en waarom ze hoe worden verwerkt. Maar ondanks deze beschrijving en uw grote wil om informatie goed te beschermen kunnen er toch verschillen van mening of disputen ontstaan. U dient er over na te denken en op te schrijven hoe u omgaat met klachten en verschillen van mening. Daarbij kan de FG en/of de AP een rol spelen. De FG is onpartijdig en u kunt bijvoorbeeld opschrijven dat u zijn advies bij een dispuut als bindend beschouwd.

Certificatie – uiteindelijk bent u er naar uw gevoel helemaal klaar voor. Uw auditors vinden dat misschien ook wel. Maar .. hoe weten anderen dat nou zeker? Daarvoor kunt u een certificering doorlopen. Dit is beschreven in artikel 42 van de AVG.

Momenteel is het nog niet helmaal helder hoe dit zal gaan werken. Er is gesproken over de noodzaak voor een "Europees zegel", maar dat is er momenteel nog niet. Wat u alvast kunt doen, mocht u certificering uiteindelijk overwegen, is eens kijken naar de ISO 27001 norm. Veel onderwerpen in de AVG kunnen worden geborgd in een informatiebeveiligingssysteem op basis van die norm.

Tenslotte: de Autoriteit Persoonsgegevens heeft een 'regelhulp' online waarin u in 10 stappen een beeld krijgt waar u aan kunt werken om goed voorbereid te zijn op de Algemene verordening gegevensbescherming:

https://rvo.regelhulpenvoorbedrijven.nl/avg/#/stappen

Over de auteur: Heinrich W. (Henk) Klöpping (1959) is gecertificeerd en geaccrediteerd informatiebeveiliger. Hij werkt als senior consultant bij Snow BV in Geldermalsen. Henk is verder actief als vrijwilliger en bestuurder binnen een aantal stichtingen.

