HANDREIKING KLANTGEGEVENS EN DE AVG: IN 10 STAPPEN AVG-PROOF

Op verzoek van uw brancheverenigingen Cultuurconnectie heeft Stadhouders Advocaten een handreiking opgesteld voor een zorgvuldige verwerking van klantgegevens in uw organisatie, culturele instelling of volksuniversiteit. In 10 stappen wordt de nieuwe Europese privacywetgeving, de AVG, doorgelopen. Per stap worden de consequenties voor uw organisatie toegelicht met praktijkvoorbeelden.[1] [2]

Inhoudsopgave:

[1] Deze handreiking bouwt voort op een aantal workshops die Stadhouders Advocaten heeft georganiseerd voor de branche. Voor de voorbeelden in deze handreiking hebben wij geput uit de discussies in de workshops.

[2] Disclaimer: Dit document is met zorg samengesteld. Het is bestemd voor de leden van de brancheverenigingen en bedoeld als algemene en praktische handreiking om de verwerking van klantgegevens in de organisatie te toetsen aan de AVG. Niet beoogd is juridisch advies te geven in concrete zaken. Stadhouders Advocaten aanvaardt geen aansprakelijkheid voor de inhoud.

Achtergrond: De AVG, hoe zit het ook alweer?

Nieuwe wetgeving privacy

Vanaf 25 mei 2018 moet het verwerken van persoonsgegevens voldoen aan de regels van de Algemene Verordening Gegevensbescherming (AVG), een Europese verordening die geldt voor elke organisatie die is gevestigd in een EU-lidstaat.

Doel AVG

Enerzijds het beschermen van persoonsgegevens, anderzijds mogelijk maken van vrij verkeer van persoonsgegevens binnen de EU. Dit vergt steeds afweging van privacy van personen en belang van degene die gegevens verwerkt.

Klantgegevens en de AVG

Klantgegevens zijn persoonsgegevens, namelijk informatie waarmee u een (potentiële) klant kunt identificeren[3], bijvoorbeeld: NAW-gegevens, geboortedatum of sommige soorten privacygevoelige cookies.[4] Deze klantgegevens zijn belangrijk voor uw organisatie. Ze zijn nodig voor een goede dienstverlening bij de verkoop van een cursus of een voorstelling, voor de nieuwsbrief en voor marketing-doeleinden. Deze klantgegevens zijn echter ook gevoelige informatie. De privacy van de klanten moet worden gewaarborgd. Het belang van de klantgegevens voor uw organisatie enerzijds en de privacy van de klanten anderzijds moeten tegen elkaar worden afgewogen. De AVG biedt daarvoor een kader.

Afwegingskader AVG

De AVG geeft *zes beginselen voor de verwerking van persoonsgegevens*[5]. Houd deze in uw achterhoofd als u klantgegevens verwerkt:

a. de verwerking moet ten aanzien van de klant *rechtmatig*, *behoorlijk* en *transparant* zijn;
b. op basis van te voren uitdrukkelijk omschreven en *gerechtvaardigde doeleinden;*
c. er mogen *niet meer gegevens* worden verwerkt *dan nodig* voor de bepaalde doeleneinden;
d. de gegevens moeten *juist zijn* en zo nodig worden geactualiseerd;
e. de gegevens mogen *niet langer* worden *bewaard dan noodzakelijk;*
f. een *passende beveiliging* (zowel organisatorisch als technisch) moet zijn gewaarborgd.

Uw belangrijkste verantwoordelijkheden op grond van de AVG

1. U moet waarborgen dat u gegevens verwerkt in overeenstemming met de AVG.
2. U moet achteraf kunnen aantonen dat uw gegevensverwerking voldoet aan de eisen uit de AVG (dit vergt dat u uw processen goed hebt gedocumenteerd (verwerkingsregister)).
3. U moet uw klanten informeren over de verwerking van uw klantgegevens (dit vergt dat u de processen aan hen kenbaar maakt (privacy-statement)).

---

[3] Als u gegevens geanonimiseerd of geaggregeerd verwerkt (gegevens zijn niet meer te herleiden tot een individu, een natuurlijk persoon) dan is de AVG niet van toepassing. Deze gegevens mag u verwerken. Als u gegevens pseudonimiseert (versleutelt) is de AVG wel van toepassing en moet de verwerking in overeenstemming gebeuren met de regels uit de AVG.

[4] Persoonsgegevens zijn alle gegevens over een geïdentificeerde of identificeerbare natuurlijke persoon: naam, adres, woonplaats, postcode, telefoonnummer, e-mailadres, foto, filmbeeld, e-mails, gegevens over iemands beroep, opleiding, meningen, ip-adres, inlogcodes, identificatienummer, bankgegevens etc.

[5] Zie artikel 5 AVG. Advies: print de AVG uit en blader hem eens door: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/verordening_2016_-_679_definitief.pdf

1. KLANTGEGEVENS: WELKE HEBT U EN WAT DOET U ERMEE?

Doel stap 1

Inzicht verkrijgen in *welke klantgegevens* u hebt, *waar en hoe u de gegevens bewaart* en *wat u ermee doet*. Ga bij elkaar zitten met sales, ICT en andere belanghebbenden. Inventariseer waar, welke, wie, wanneer en hoe lang gebruik maakt van klantgegevens in de organisatie.

Welke?

Beoordeel tot *welk type persoonsgegevens* uw klantgegevens behoren. We onderscheiden 3 typen persoonsgegevens: *gewone*, *bijzondere*[6] en *strafrechtelijke gegevens*.[7] Voor het mogen verwerken van elk type gelden verschillende grondslagen. Ga er voor uw branche maar vanuit dat u deze bijzondere en strafrechtelijke persoonsgegevens *niet* mag verwerken.

Waar en hoe lang?

Klantgegevens komen op verschillende manieren de organisatie binnen (via de website (via cookies of cursusinschrijving), via de ledenadministratie, andere organisaties etc.). Vervolgens worden de klantgegevens opgeslagen voor gebruik (administratie, nieuwsbrief, archief, debiteurenbeheer, klantanalysebestanden, etc). Hoe lang worden de gegevens op dit moment bewaard? Inventariseer en beschrijf deze trajecten.

Waarvoor ?

Waarvoor gebruikt u de klantgegevens (verkoop, marketing, analyse)? Inventariseer en beschrijf.

Wie?

Wie heeft toegang tot de klantgegevens en wie maakt gebruik van de klantgegevens (sales, directie, stagiaires)? Worden de gegevens gedeeld met de derde partijen (ict-provider, website-provider, drukker van nieuwsbrief, andere gemeentelijke instellingen)? Inventariseer en beschrijf.

Resultaat stap 1

U weet waar zich de klantgegevens zich bevinden, wie toegang heeft, wanneer ze worden gebruikt (dus met *welk doel* u de gegevens verwerkt) en hoe lang u de gegevens bewaard. U weet dat u geen bijzondere en strafrechtelijk persoonsgegevens mag verwerken (deze moeten uit uw verwerkingssystemen). Dit zijn de bouwstenen voor de analyse en vormen een opmaat voor het *verwerkingsregister* (zie stap 7) en in het *privacy-statement* (zie stap 9).

Voorbeeld inventarisatie/beschrijving klantgegevens					
Activiteit	**Welke klantgegevens**	**Vindplaats (waar, hoe lang)**	**Waarvoor (doel)**	**Wie heeft toegang**	**Delen met derden**
Bijv. Verkoop cursus	Bijv. NAW, Bankgegevens	Bijv. Ledenadministratie ICT provider Eeuwig	Bijv. Cursusverkoop	Bijv. Medewerkers marketing balie, directie	Bijv. Facebook, ICT, Administratie Drukker,

[6] Bijzondere persoonsgegevens zijn door hun aard bijzonder gevoelig en worden in de AVG extra beschermd. Het verwerken van bijzondere persoonsgegevens is verboden, tenzij u zich kunt beroepen op een wettelijke uitzondering. Bijzondere persoonsgegevens zijn gegevens over ras of etnische afkomst (bedenk dat geboorteplaats hieronder kan vallen), politieke opvattingen, levensbeschouwelijke overtuiging, lidmaatschap vakvereniging, gezondheid, seksuele geaardheid, genetische gegevens, biometrische gegevens).

[7] Het verwerken van strafrechtelijke persoonsgegevens is verboden, tenzij u zich op een specifieke wettelijke uitzondering kunt beroepen.

2. BENT U VERANTWOORDELIJKE OF VERWERKER?

Doel stap 2

U zoekt uit of u verantwoordelijke bent of verwerker op basis van de uitkomst van stap 1 (u bent nagegaan met welke partijen u samenwerkt om gegevens te verwerken).

Wat is het onderscheid?

De verantwoordelijke stelt het doel en de middelen voor verwerking vast. De verwerker verwerkt persoonsgegevens ten behoeve van de verantwoordelijke (denk aan factureringsbedrijven, drukkers). De AVG stelt aan beide profielen andere eisen. Als verantwoordelijke hebt u meer taken en verantwoordelijkheden op grond van de AVG en daarbij geldt een ruimere aansprakelijkheid ten aanzien van schade die u wegens overtreding van de AVG hebt veroorzaakt.

Verantwoordelijke?

Wanneer uw organisatie het doel (organisatie van een cursus of evenement, marketing, etc.)[8] en de middelen (docenten, locatie, ledenadministratie, facturatie, website, drukker, etc.) voor de verwerking van de klantgegevens vaststelt, is uw organisatie aan te merken als verantwoordelijke. Dat zal in de meeste gevallen zo zijn, denken wij.

Verwerker?

Als verwerker zullen in dit geval zijn aan te merken: docenten, de ict- en website provider, de drukker etc.. Is sprake van samenwerking met een verwerker: leg afspraken vast in een *verwerkersovereenkomst*.[9] L

> **Voorbeeld:**
> Uw organisatie, normaal gesproken verwerkingsverantwoordelijke, kan in sommige gevallen ook verwerker zijn, wanneer uw organisatie in opdracht van een docent een zaal verhuurt voor een cursus en slechts beschikt over klantgegevens om extra service te kunnen bieden (b.v. locatie leslokalen doorgeven).
> **Let op:** de docent is in deze situatie dus verantwoordelijk voor de verwerking van de gegevens en dient in dat verband te voldoen aan de eisen van de AVG!

Twee of meer verwerkingsverantwoordelijken

Er kan sprake zijn van een gedeelde verantwoordelijkheid waarbij twee of meer organisaties het doel en de middelen van de verwerking bepalen. Is sprake van samenwerking tussen twee of meer verantwoordelijken: leg afspraken schriftelijk vast in een *samenwerkingsovereenkomst*.[10]

> **Voorbeeld:**
> Uw organisatie biedt in samenwerking met een docent een cursus aan. Organisatie en docent verzorgen gezamenlijk de verkoop en delen klantgegevens. Afhankelijk van de omstandigheden zijn uw organisatie en de docent dan gedeelde verwerkingsverantwoordelijken.

Resultaat stap 2

U weet of u *verwerkingsverantwoordelijke of verwerker* bent. U weet of u samen met anderen verwerkingsverantwoordelijke bent en als dat het geval is, sluit u een *samenwerkingsovereenkomst*. U weet wie uw verwerkers zijn en zorgt dat u met elk van hen een *verwerkersovereenkomst* sluit. U moet zich ervan vergewissen dat organisaties of docenten met wie u gegevens deelt ook zelf voldoen aan de eisen uit de AVG.

---

[8] Zie uitkomst stap 1.
[9] Bijvoorbeeld: onderwerp, aard, duur en doel van de verwerking, soort klanten, en uw rechten als verwerkingsverantwoordelijke, instructies over de verwerking, geheimhoudingsplicht, beveiliging, subverwerking, privacy-rechten van klanten, datalekken, meewerken aan audits
[10] Bijvoorbeeld: wie heeft welke rol/taak, wie is waarvoor verantwoordelijk, hoe worden klanten geïnformeerd?

3. ZIJN DE VERWERKINGEN DIE U WILT UITVOEREN RECHTMATIG?

Doel stap 3

De verwerking van klantgegevens moet u kunnen baseren op tenminste één van de 6 in de AVG opgesomde grondslagen. Als u dat niet kunt, is de verwerking in strijd met de AVG en onrechtmatig. Dan moet u daarmee stoppen. Voor uw branche zijn bij verwerking van klantgegevens vier van de zes grondslagen relevant.[11] Deze vier komen achtereenvolgens aan de orde.

Grondslag: uitvoering overeenkomst

Als u een overeenkomst heeft, mag u de verwerking van persoonsgegevens die nodig zijn voor de uitvoering hiervan op deze grondslag baseren.[12]

Aan veel van de verwerkingen van klantgegevens in uw organisatie zal dezelfde soort overeenkomst ten grondslag liggen, namelijk de koopovereenkomst (cursus). Op basis van deze koopovereenkomst verwerkt u de klantgegevens in verschillende facetten van het koopproces: administreren, betaling, services-mails, etc.

Bij de verwerking van de klantgegevens zult u zich niet altijd op een koopovereenkomst kunnen beroepen. In dat geval moet u onderzoeken op welke grondslag u de verwerking kunt baseren. Wij zien in de praktijk de volgende voorbeelden:

Voorbeelden:

- De verwerking valt buiten de uitvoering van de koopovereenkomst. Denk aan klantonderzoek, archief, klantprofielen aanleggen, direct marketing (mailings) etc.
- De koopovereenkomst bestaat (nog) niet. De klant heeft zich nog niet ingeschreven voor cursus, maar wil een nieuwsbrief ontvangen.
- De verwerking gebeurt in opdracht van het openbaar gezag, bijv. de gemeente of brandweer.

Grondslag: gerechtvaardigd belang

Deze grondslag vergt een afweging tussen de gerechtvaardigde belangen van uw organisatie en de gevolgen voor de belangen en rechten van de betrokkene. In deze afweging wordt ook betrokken in hoeverre er maatregelen zijn genomen om onnodige inbreuk op de privacy te voorkomen. Voor een beroep op deze grondslag moet u dus voldoen aan drie voorwaarden:
1) u heeft een gerechtvaardigd belang (in het kader van reguliere bedrijfsactiviteiten),
2) de verwerking is noodzakelijk om dit gerechtvaardigde belang te behartigen, en
3) u heeft een afweging gemaakt tussen uw belangen en die van de personen van wie u persoonsgegevens verwerkt.

Voorbeeld:

Een klant schrijft zich in voor een cursus en laat daarvoor zijn e-mailadres achter. Een paar maanden later stuurt u per e-mail een aanbieding voor een vergelijkbare cursus.
Uw organisatie lijkt hiervoor een gerechtvaardigd, maar niet bijzonder zwaarwegend, belang te hebben bij het verkopen van meer cursussen aan uw klanten. Aan de andere kant lijkt de inbreuk op privacy van de klant in dit geval niet heel groot. De gebruikte gegevens en de context lijkt op het eerste gezicht niet heel privacygevoelig (cursussen). Uw organisatie gebruikt relatief weinig persoonsgegevens (e-mailadres). Daarnaast is het belangrijk of uw organisatie de vereiste veiligheidsmaatregelen heeft getroffen: a) een opt-out voor dit soort mailings bij inschrijving voor de cursus, b) opt-out in mailing zelf, c) beperkt aantal mailings en d) de vereiste transparantie door een duidelijk privacy-statement. Met andere woorden: het is

---

[11] De resterende grondslagen lijken voor de dagelijkse praktijk bij de verwerking van klantgegevens in uw branche niet relevant, namelijk a) ter vrijwaring vitaal belang betrokkene en b) nodig voor goede vervulling publiekrechtelijke taak. U zult het moeten doen met de vier genoemde grondslagen.
[12] De overeenkomst zelf kan niet gericht zijn op het verwerken van persoonsgegevens, maar moet een ander doel hebben.

een complexe belangenafweging die in elk geval anders kan uitvallen. Als u expliciet toestemming vraagt aan de klant, heeft u deze onzekerheid niet.

Onder welke omstandigheden een organisatie een geslaagd beroep kan doen op deze grondslag, is onzeker en nog niet uitgekristalliseerd. Dit geldt zeker voor de verwerking van klantgegevens. Als uw organisatie een beroep wilt doen op deze grondslag, adviseren wij dit te laten toetsen.

Grondslag: toestemming van de klant

Als de betrokkene toestemming geeft, is het toegestaan om persoonsgegevens te verwerken. Dit klinkt eenvoudig, maar de AVG stelt verschillende zwaarwegende eisen aan het verkrijgen van deze toestemming.

Vereisten toestemming:

- u moet kunnen *aantonen dat toestemming is gegeven*; mondelinge toestemming zorgt dus voor bewijsproblemen;
- de toestemming moet *vrijelijk gegeven* zijn: u mag iemand dus niet onder druk zetten, bijvoorbeeld door nadelige gevolgen te verbinden aan het weigeren van toestemming;
- de toestemming moet *ondubbelzinnig gegeven* zijn;
- toestemming moet gelden voor een *specifieke verwerking* en een *specifiek doel*: als de verwerking meerdere doeleinden heeft, dient u de klant hierover te informeren en voor elk doel afzonderlijk toestemming te vragen. Het doel mag niet gaandeweg veranderen;
- verzoek om toestemming moet *begrijpelijk in duidelijke en eenvoudige taal* worden gepresenteerd en er moet een *duidelijk onderscheid zijn met andere aangelegenheden*;
- toestemming moet even *eenvoudig zijn in te trekken* als het geven ervan;
- de toestemming is niet geldig als u die als voorwaarde stelt voor het aangaan van een overeenkomst waarvoor u de *gegevens niet nodig* hebt;
- de klant moet tevoren zijn *geïnformeerd* (zie onder stap 9) AVG schrijft niet voor in welke vorm toestemming moet worden gevraagd (d.m.v. handtekening of aankruisen vakje of nog anders).
  Let op: toestemming bij kinderen. De AVG beschermt kinderen jonger dan 16 jaar extra. Zij kunnen de risico's van gegevensbescherming minder goed inschatten. Om gegevens van hen te mogen verwerken moet er toestemming zijn van degene die gezag over hen heeft;

Voorbeeld:

Iemand wil zich aanmelden voor de nieuwsbrief van uw organisatie en is nog geen klant. Zij kan haar e-mailadres achterlaten op de betreffende plek op de website. Zij geeft daarmee toestemming voor het ontvangen van de nieuwsbrief. Deze toestemming moet in uw administratie worden vastgelegd. De toestemming moet eenvoudig in te trekken zijn door in de nieuwsbrief de mogelijkheid op te nemen dat zij zich kan afmelden.
Let op: De kans is groot dat uw organisatie op dit moment voor de nieuwsbrief nog het gehele adressenbestand gebruikt, zonder dat duidelijk is of deze personen in het verleden toestemming hebben gegeven voor het gebruik van hun gegevens voor deze verwerking. Als dat zo is, dient u te overwegen om door een nieuwe mailing alsnog toestemming te verkrijgen van deze personen. Als uw nieuwsbrief al lange tijd over een afmeldoptie beschikt, zou u ook kunnen overwegen om met een beroep op de andere grondslag "gerechtvaardigd belang" deze mailing voort te zetten. Kennelijk willen deze klanten de nieuwsbrief wel ontvangen. Deze laatste keuze vergt vanzelfsprekend de bovengenoemde belangenafweging. Ook dient u te waarborgen dat bij aanmeldingen van nieuwe personen de toestemming wel wordt gevraagd. Ook hier geldt: met toestemming geeft u een grotere zekerheid dat de verwerking een wettelijke grondslag heeft.

Grondslag: uitvoering wettelijke verplichting
Het verwerken van klantgegevens zal alleen in uitzonderlijke gevallen gebaseerd kunnen worden op een wettelijke verplichting.

> **Voorbeeld:**
> Uw organisatie heeft op last van de brandweer een lijst van in het gebouw aanwezige gasten bij de balie liggen.

Resultaat van stap 3
U hebt vastgesteld of uw verwerkingen rechtmatig zijn, dat wil zeggen of zij berusten op een of meer van de zes in de AVG opgesomde grondslagen. Indien u heeft vastgesteld dat uw verwerkingen niet berusten op een van de zes grondslagen, beëindigt u een dergelijke verwerking.
De grondslagen van uw verwerkingen kunt u op nemen in het *verwerkingsregister* (zie stap 7) en in het *privacy-statement* (zie stap 9).

4. WIE WORDT VERANTWOORDELIJK VOOR PRIVACY IN UW ORGANISATIE?

Doel stap 4
U weet wat de functie is van een functionaris gegevensverwerking en of u deze moet aanstellen.

Wat is een functionaris gegevensbescherming?
Een Functionaris gegevensbescherming (FG) is iemand die binnen uw organisatie toezicht houdt op de toepassing en naleving van de AVG.

> **Voorbeeld werkzaamheden:**
> - toezicht houden;
> - inventarisaties van gegevensverwerkingen maken;
> - meldingen van gegevensverwerkingen bijhouden;
> - vragen en klachten van mensen binnen en buiten de organisatie afhandelen;
> - interne regelingen ontwikkelen;
> - adviseren over technologie en beveiliging (privacy by design);
> - input leveren bij het opstellen of aanpassen van een gedragscode.

Wettelijke vereisten FG:
- De FG is een natuurlijk persoon. De OR of een commissie komt dus niet in aanmerking.
- Een FG moet voldoende kennis hebben van de organisatie en de privacywetgeving.
- Een FG moet betrouwbaar zijn. Dit uit zich onder meer in een geheimhoudingsplicht.

Bevoegdheden FG:
- Een FG heeft geen formele sanctiebevoegdheden. Maar uw organisatie is wel wettelijk verplicht om de FG controlebevoegdheden te geven (bevoegdheid toetreding ruimtes, onderzoek zaken en vragen inlichtingen en inzage).
- Een FG moet in onafhankelijkheid zijn werkzaamheden kunnen verrichten binnen uw organisatie.
- Een FG heeft dezelfde ontslagbescherming als leden van een ondernemingsraad. Dit betekent dat hij pas ontslagen kan worden na toestemming van de kantonrechter.

Bent u verplicht tot aanstellen van een FG?
Een FG is verplicht voor:
- overheidsinstanties;
- organisaties die bijzondere en/of strafrechtelijke persoonsgegevens verwerken;
- organisaties die regelmatige of stelselmatige observaties van personen als kernactiviteit hebben, voorbeelden hiervan:

- het volgen en profileren van internetgebruikers;
- zoekmachine die persoonsgegevens verwerkt om advertenties te kunnen tonen op basis van internetgedrag.

Op grond van deze criteria bent u waarschijnlijk niet verplicht een FG aan te stellen, maar u moet dit voor uzelf goed beoordelen. Stelt u geen FG aan? Zorg er in elk geval voor dat u goed kunt onderbouwen waarom u daarvoor kiest.

Niet verplicht, toch aanstellen FG?

Met het oog op de implementatie van de AVG en de groeiende aandacht voor privacy en het feit dat u veel persoonsgegevens van derden (klanten) verwerkt, geven wij uw organisatie in overweging om iemand in uw organisatie aan te wijzen als FG. Een FG kan ook voor meerdere organisaties werken.

Resultaat stap 4

U weet of u een FP aan moet stellen. Indien u een FP aanstelt, meldt u deze aan bij de AP, u vermeldt de contactgegevens in het *verwerkingsregister* (zie stap 7) en in het *privacy-statement* (zie stap 9). Indien u geen FP aanstelt, motiveert u dat in uw verwerkingsregister zodat u deze keuze indien nodig kunt verantwoorden aan de AP.

5. BENT U VERPLICHT EEN DPIA UIT TE VOEREN?

Doel stap 5

U moet bij deze stap een inschatting maken of uw gegevensverwerkingen een hoog privacy-risico opleveren voor de personen van wie u persoonsgegevens verwerkt. Als dat zo is, bent u verplicht om een DPIA uit te voeren.

Wat is een DPIA?

De data protection impact assessment (DPIA) is een instrument om vooraf de privacy-risico's van gegevensverwerking in kaart te brengen en vervolgens maatregelen te nemen om de risico's te verkleinen.

Bent u verplicht een DPIA uit te voeren?

Een DPIA kan bijvoorbeeld verplicht zijn als u gebruik maakt van gekoppelde database, als u big data gebruikt voor profiling of als u gevoelige gegevens van zeer persoonlijke aard verwerkt. [13]

Uw organisatie zal bij de klantgegevens waarschijnlijk beperkte gegevens verwerken (naam, adresgegevens, e-mailadres, telefoon, mogelijk ook persoonlijke interesses).
Deze gegevens verwerkt u hoofdzakelijk voor de verkoop van cursussen. Dit betekent dat er waarschijnlijk geen sprake is van een hoog privacyrisico. In dat geval hoeft u geen DPIA uit te voeren. Als u besluit om geen DPIA uit te voeren, zorg dan dat u motiveert en documenteert waarom niet. U moet dit kunnen verantwoorden aan de Autoriteit Persoonsgegevens (AP).

Resultaat stap 5

U hebt een inschatting gemaakt van de privacy-risico's van uw verwerkingen. Zijn die hoog dan laat u een DPIA uitvoeren. De resultaten van de DPIA verwerkt u in uw processen. Als u besluit om geen DPIA uit te voeren, dan motiveert en documenteert u waarom niet en neemt dat op in het *verwerkingsregister* (zie stap 7) zodat u deze keuze indien nodig kunt verantwoorden aan de AP.

[13] Tot de laatste categorie behoren de bijzondere persoonsgegevens. Het kan echter ook gaan om gegevens over iemands beroepsprestaties, economische situatie en financiële gegevens, gezondheid, persoonlijke voorkeuren of interesses, locatie of verplaatsingen, privé-activiteiten, BSN-nummer, wachtwoorden etc.

6. VOLDOET U AAN DE EISEN VAN PRIVACY BY DESIGN EN DEFAULT ?

Doel stap 6

Doel is dat u beide concepten begrijpt en zoveel mogelijk integreert in uw diensten en producten. In het bijzonder wordt ingegaan op de bewaartermijn.

Wat is privacy by design en default?

Privacy by Design (ontwerp) is voornamelijk van toepassing op de ontwerpfase van (nieuwe) producten en diensten. *Privacy by Default* (standaardinstelling) ziet op producten of diensten waarbij gebruikers zelf de mogelijkheid wordt geboden om persoonsgegevens te delen of af te staan (meestal bij een bezoek op websites of bijvoorbeeld via apps). Het concept van Privacy by Default verplicht organisaties om de privacy van hun gebruikers te beschermen door instellingen en functies van de producten of diensten standaard (by default) op de meest privacyvriendelijke stand te zetten. Zowel op technisch (IT) als organisatorisch niveau moet u maatregelen treffen om de privacy-risico's voor mensen zo klein mogelijk te houden. Uitgangspunt daarbij is dataminimalisatie en zo mogelijk pseudonimiseren van klantgegevens.

Voorbeelden

- zijn uw producten, diensten en systemen standaard privacyvriendelijk ontworpen?
- heeft u bepaald hoe lang u persoonsgegevens gaat bewaren en/of criteria voor de bewaartermijn bepaald?
- worden gegevens automatisch verwijderd als de bewaartermijn voorbij is?
- staan de instellingen op privacyvriendelijk?
- hebt u bepaald wie er in uw organisatie wel of geen toegang krijgen tot de gegevens?

Bewaartermijn?

De bewaartermijn voor persoonsgegevens mag niet langer zijn *dan noodzakelijk voor het gegeven doel*. Het doel van het bewaren van de persoonsgegevens kan verschillen per activiteit. De noodzakelijke bewaartermijn zal per activiteit verschillen. Voor elke activiteit is daarom een afzonderlijke afweging noodzakelijk.

De volgende wettelijke bewaartermijnen geven bij deze afweging voor klantgegevens enige houvast:

- Bewaartermijn fiscale boekhoud- en administratieplicht = 7 jaar (art. 52 AWR)

Bewaarplicht voor administraties bij boekjaarsubsidies (optioneel) = 7 jaar (art. 4:69 Awb)

Daarnaast kent het Vrijstellingsbesluit Wet bescherming persoonsgegevens voor klantgegevens concrete handvatten:

- Bewaartermijn voor persoonsgegevens bij dienstverlening = 2 jaar nadat de desbetreffende transactie is afgehandeld (art. 13 lid 5 Vrijstellingsbesluit).

Wat betekent dit voor uw organisatie?

Hieronder een paar voorbeelden voor het bepalen van de bezwaartermijn voor de verwerking van klantgegevens voor zover noodzakelijk voor het specifieke doel.

Voorbeelden:

- Nieuwsbrief: dit lijkt een voortdurende dienstverlening. De bewaartermijn lijkt dus niet beperkt.[14] Voorwaarden zijn wel: minimaal gebruik persoonsgegevens (bijv. alleen e-

[14] Aangenomen dat u de nieuwsbrief minimaal eenmaal in de twee jaar verstuurt (zie indicatie Vrijstellingenbesluit).

mailadres en naam bij e-mailnieuwsbrief), een afmeldoptie is aanwezig en vastlegging toestemming van de klanten.

- Verkoopadministratie: maximale bewaartermijn lijkt twee jaar nadat het *laatste* cursus is gekocht (indicatie Vrijstellingenbesluit). Deze termijn zal uw organisatie als kort ervaren. Als u een langere termijn kiest, moet u dat goed kunnen motiveren. U moet kunnen aantonen dat de gekozen termijn noodzakelijk is voor het doel waarvoor u de klantgegevens bewaart.
- Boekhouding: u dient de facturen te bewaren tot zeven jaar op grond van de wettelijke bewaartermijn.
- Subsidieadministratie: het lijkt niet noodzakelijk om de klantgegevens voor dit doel zeven jaar te bewaren. De subsidieverstrekker zal geen contractuele of wettelijke grondslag hebben om inzage in de klantgegevens te vorderen.
- Klantenanalyse: als uw organisatie elke vijf jaar een analyse van het klantenbestand maakt, kan dat een rechtvaardiging zijn om de klantgegevens langer te bewaren. Uw organisatie dient dan wel een afweging te maken of het bewaren van het gehele bestand in de normale klantenadministratie geen onevenredige inbreuk maakt op de privacy van de klanten. U dient beveiligingsmaatregelen te nemen: bijv. het bestand apart te zetten en/of te pseudonimiseren (stap 8).

Resultaat stap 6

U hebt ervoor gezorgd dat de privacy van uw klanten van ontwikkeling tot aan het laatste gebruik zoveel mogelijk is geïntegreerd in uw diensten en producten. Het gaat hier om maatwerk. Beschrijf de ondernomen stappen en neem deze op in het Verwerkingsregister (zie onder stap 7). U heeft voor alle klantgegevens een bewaartermijn bepaald en past die toe.

7. HOE LEGT U VERANTWOORDING AF?

Doel stap 7

Het opstellen van een register van verwerkingsactiviteiten is onder de AVG vaak een verplichte maatregel. Of u zo'n register moet opstellen, hangt af van de omvang van uw organisatie én van het type gegevens dat u verwerkt.

Wat is het register?

Er wordt een onderscheid gemaakt tussen twee soorten registers. Een register van de structurele verwerkingen en een register van de incidentele verwerkingen van klantgegevens. Het register heeft als doel dat uw organisatie de gegevensverwerking kan verantwoorden aan bijvoorbeeld de AP, wanneer daarom wordt verzocht.

Is een register verplicht?

Heeft uw organisatie meer dan 250 medewerkers? Dan is een register verplicht.
Heeft uw organisatie minder dan 250 medewerkers? Dan is een register verplicht als u persoonsgegevens verwerkt:
- waarvan de verwerking niet incidenteel is (verwerkingen zijn zelden incidenteel, denk aan verwerken van klantgegevens)
- die een hoog risico inhouden voor de rechten en vrijheden van de betrokkenen (denk aan de gevoelige informatie zoals omschreven onder punt 5)
- die vallen onder de categorie bijzondere persoonsgegevens (zoals opgesomd onder 1)

Onze inschatting is dat uw organisatie verplicht is tot het opstellen en bijhouden van een verwerkingsregister. Het gaat dan om een verwerkingsregister van de structurele verwerkingen, niet van de incidentele verwerkingen.

Inhoud register?

Een *verwerkingsverantwoordelijke* moet de volgende informatie opnemen in het register:[15]

- naam en contactgegevens van uw organisatie en van medeverantwoordelijke organisaties;
- naam en contactgegevens FG (als u die hebt aangesteld);
- doelen waarvoor u persoonsgegevens verwerkt;
- beschrijving van de categorieën van personen van wie u gegevens verwerkt;
- beschrijving van de categorieën van persoonsgegevens;
- bewaartermijn van de gegevens;
- categorieën van ontvangers aan wie u persoonsgegevens verstrekt;
- delen van gegevens met organisaties buiten de EU;
- beschrijving van technische en organisatorische maatregelen voor beveiliging van gegevens.

Resultaat van stap 7

U hebt een verwerkingsregister opgesteld. De tabel opgesteld in stap 1 vormt daarvoor de opmaat.

8. ZIJN UW KLANTGEGEVENS VOLDOENDE BEVEILIGD?

Doel stap 8

U neemt kennis van de noodzaak van de beveiligingsmaatregelen en de wijze waarop u daar invulling aan geeft.

Uitgangspunten

In de AVG staat dat u persoonsgegevens goed moet beveiligen. De AVG noemt vier typen maatregelen die u, indien passend, moet nemen:

- de pseudonimisering (versleuteling) van persoonsgegevens
- zorgen voor permante waarborg van vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten.
- tijdig kunnen herstellen van de toegang tot gegevens bij een incident
- procedure voor regelmatige testen, beoordelen en evalueren van doeltreffendheid van de technisch en organisatorische maatregelen ter beveiliging van de verwerking

Technische en organisatorische maatregelen

Beveiliging geldt *op technisch niveau,* voorbeelden: (logische en fysieke (toegangs-) beveiliging en beveiliging van apparatuur (firewalls en netwerksegregatie), bijhouden van logbestanden, zo beperkt mogelijke autorisaties, software zoals virusscanners en browsers up-to date houden, back-ups maken, automatische verwijdering van verouderde gegevens, versleutelen, minder gegevens verwerken op uw servers en meer gegevensverwerkingen laten plaatsvinden op de apparatuur van de gebruiker, beveiligen met HTTPS, laten testen van uw systemen, etc.

Beveiliging vindt daarnaast plaats *op organisatorisch niveau,* voorbeelden: toewijzen van verantwoordelijkheden voor informatiebeveiliging, voorlichten van personeel, opstellen van procedures om op gezette tijden de beveiligingsmaatregelen te testen, regelmatige controle logbestanden, protocol opstellen voor datalekken en beveiligingsincidenten, sluiten van geheimhoudingsafspraken (in bijv. verwerkersovereenkomsten), beoordelen of doelen kunnen worden bereikt met minder persoonsgegevens, minder mensen toegang geven tot gegevens.

---

[15] In het verwerkingsregister van een verwerker moet de volgende informatie staan
- contactgegevens van de organisatie en van de verwerkingsverantwoordelijke
- gegevens van de FG als die is aangesteld
- beschrijving van de categorieën van verwerkingen die in opdracht van iedere verantwoordelijke uitvoert.

Wat betekent dat voor u?

Uw beveiligingsniveau moet zijn afgestemd op de risico's die de gegevensverwerking met zich meebrengt. Het is een continu proces. Uitgangspunten daarbij zijn de stand van de techniek, de uitvoeringskosten, de aard, de omvang en de verwerkingsdoeleinden van de verwerking en hoe waarschijnlijk en ernstig het is voor de betrokken personen als er een beveiligingslek ontstaat.

Resultaat stap 8

U hebt een voor uw organisatie passende beveiliging voor persoonsgegevens die u verwerkt, zowel technisch als organisatorisch. U omschrijft de gezette stappen en u omschrijft de wijze waarop u de veiligheid regelmatig test en evalueert. U neemt dit op in uw verwerkingsregister (zie stap 7).

9. HOE INFORMEERT U KLANTEN DOELTREFFEND?

Doel stap 9

U neemt kennis van de noodzaak uw klanten te informeren over de verwerking van hun gegevens en de wijze waarop u daar vorm aangeeft.

Wat houdt de informatieplicht in: een privacy-statement?

Een belangrijk uitgangspunt van de AVG is dat het verwerken van persoonsgegevens transparant dient te zijn voor de betrokkenen. Mensen hebben het recht om te weten wat er met hun persoonsgegevens gebeurt. U bent verplicht om klanten op een begrijpelijke manier te informeren welke gegevens u voor welk doel en met welke grondslag verzamelt en verwerkt. Ook bent u verplicht om betrokkenen te informeren over hun rechten op grond van de AVG.

Inhoud privacy-statement

U dient daarom een privacy-statement (privacyverklaring) op te stellen, met in elk geval de volgende informatie:

1. De identiteit en de contactgegevens van de verwerkingsverantwoordelijke;
2. De contactgegevens van de FG als u die heeft;
3. De doeleinden en rechtsgrond van de verwerking, en als u zich beroept op een gerechtvaardigd belang: op welk belang u zich beroept;
4. De (categorieën van) ontvangers van de persoonsgegevens;
5. Of u van plan bent de persoonsgegevens door te geven buiten de EU;
6. De bewaartermijn van de gegevens;
7. De rechten van de betrokkene, zoals het recht op inzage, correctie en verwijdering;
8. Het recht van de betrokkene om de gegeven toestemming voor een bepaalde verwerking altijd in te kunnen trekken;
9. Dat de betrokkene een klacht kan indienen bij de AP;
10. Of en waarom de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de gevolgen zijn als de gegevens niet worden verstrekt;
11. Of u gebruik maakt van geautomatiseerde besluitvorming, inclusief profilering, en hoe u besluiten neemt;
12. Als de gegevens van een andere organisatie zijn verkregen: de bron waar de persoonsgegevens vandaan komen, en in voorkomend geval, of zij afkomstig zijn van openbare bronnen;

Resultaat stap 9

U hebt een privacy statement opgesteld zodat u voldoet aan de informatieplicht jegens uw klanten.

10. BENT U VOORBEREID OP PRIVACY-AANSPRAKEN VAN KLANTEN?

Doel stap 10

U zorgt dat uw organisatie is voorbereid op privacy-aanspraken van klanten.

Rechten van uw klanten

Betrokkenen hebben onder de AVG de volgende rechten:

- Recht op inzage;
- Recht op rectificatie en aanvulling;
- Recht op vergetelheid (op verzoek van de klant gegevens wissen);
  Dit recht geldt niet altijd. Het is onder meer van toepassing als u de gegevens niet meer nodig hebt voor het doel waarvoor u ze hebt verzameld, als eerder gegeven instemming wordt ingetrokken, als u persoonsgegevens op onrechtmatige wijze verwerkt, als bezwaar wordt gemaakt tegen direct marketing, als u gegevens te lang bewaart
- Recht op dataportabiliteit;
- Recht op beperking van de verwerking;
- Rechten met betrekking tot geautomatiseerde besluitvorming en profilering;
- Recht van bezwaar.

Resultaat stap 10

U hebt uw systemen, procedures en interne organisatie op deze rechten ingericht zodat u op de juiste manier gehoor kunt geven aan verzoeken van klanten die deze rechten uitoefenen.

JURIDISCHE CHECK, VRAGEN, OPSTELLEN REGISTER/PRIVACY-STATEMENT OF CONTRACTEN?

We hebben inmiddels ervaring met het op maat uitwerken van register gegevensverwerkingen, privacy statements, verwerkers- en samenwerkingsovereenkomsten voor de branche. Voor vragen, bel Stadhouders Advocaten (Martine ten Voorde of Clemens Mesker: 030-2520855 of mail: tenvoorde@stadhouders.nl of mesker@stadhouders.nl). Stadhouders Advocaten adviseert u graag nader over de AVG!