Taskforce Samenwerkingsverband Publieksdata

Publieksdata & de AVG

Waar moet je rekening mee houden?

Juli 2022, v.1.0

Door: Femke Luijkx, advocaat

Doe meer met Publieksdata

Inhoud

Inleiding

Beste lezer,

Dit naslagwerk is bestemd voor de culturele sector, in het bijzonder de kleinere en middelgrote organisaties, en beoogt meer inzicht en duidelijkheid te verschaffen over de toepassing van de AVG. Het is gebleken dat hier binnen de sector veel behoefte aan is.

De AVG is in 2018 in werking getreden, als opvolger van de Wet Bescherming Persoonsgegevens. Sindsdien zal elke organisatie stappen hebben gezet om deze privacywetgeving te implementeren. Het onderwerp staat sindsdien (als het goed is) blijvend op de agenda om ook binnen jouw organisatie privacy naar een volgend niveau te tillen. Daarnaast digitaliseert de maatschappij steeds verder en daarbij zullen ook telkens nieuwe privacyvragen moeten worden beantwoord.

De bescherming van een privéleven en van persoonsgegevens is een grondrecht voor ieder mens. Binnen Europa is met de AVG gekozen voor een gelijk en hoogwaardig beschermingsniveau met meer rechten voor de betrokkenen. Met ontwerprichtlijnen op het gebied van AI en bijvoorbeeld Platformarbeid blijft de EU constant bezig om de burgers en interne markt zo goed en duurzaam mogelijk te beschermen, ook naar de toekomst toe.

Het respecteren en waarborgen van privacy is belangrijk en waardevol voor je organisatie. Een datalek of slordige omgang met persoonsgegevens kan grote reputatieschade opleveren. Nog los van het strenge toezicht dat de Autoriteit Persoonsgegevens uitvoert. Deze werkt met hoge boetes en "*naming and shaming*". Geen prettig vooruitzicht. Gelet op de toenemende digitalisering, kun je ervan uitgaan dat de waarde en impact van goed gewaarborgde privacy alleen maar zal toenemen. Voor bestuurders en directie zal behoefte bestaan aan risicomanagement, weten waar er risico's worden gelopen en het terugbrengen naar aanvaardbare proporties daarvan. Ook voor de medewerkers is het een belangrijk en positief signaal dat de werkgever op verantwoorde wijze omgaat met privacy.

Bij veel organisaties bestaat de behoefte om meer met data te doen, of een breder publiek te bereiken. Ook zal er wellicht binnen de organisatie nog *old school* worden omgegaan met data en/of het benaderen van je publiek. Hoe wil de organisatie zich gaan opstellen in de digitale wereld? Als culturele instelling wil je de privacy van de bezoekers respecteren en bijdragen aan een veilige digitale omgeving. Tegelijkertijd wil je het publiek interesseren voor de mooie voorstellingen of tentoonstellingen die op het programma staan. Hoe breng je dit in balans? Tijd om een volgende slag te maken met privacy!

Dit naslagwerk is bedoeld om de belangrijkste aspecten van het onderwerp privacy praktisch toepasbaar te maken. Hopelijk helpt dit naslagwerk een eind op weg bij de omgang met persoonsgegevens en in het bijzonder publieksdata. Het is echter niet de intentie om volledig te zijn of op alles een antwoord te geven. De basics zijn in dit naslagwerk grotendeels gecoverd en voor verdiepende stof zijn enkele verwijzingen opgenomen. Daarnaast is de website van de Autoriteit Persoonsgegevens (AP) ook een prima startpunt om tips en handreikingen te vinden.

De Taskforce Samenwerkingsverband Publieksdata heeft er alle vertrouwen in dat deze notitie bijdraagt aan een veilige en verantwoorde omgang met publieksdata binnen de culturele sector.

1. Stappenplan

1. Voor een effectieve aanpak van privacy door de gehele organisatie is het belangrijk om een privacyteam en/of -stuurgroep te formeren. Zorg voor diverse expertise (compliance, ICT, marketing of andere commerciële rol). Dit team en de privacycoördinator zijn aanspreekbaar voor privacyvragen en leggen alle acties vast (accountability, compliance)
2. Privacycoördinator: in de AVG wordt veel sterker belang gehecht aan "compliance"[1]: planning en control, en het aantoonbaar voortdurend blijven werken aan privacy. Wijs daarom een privacycoördinator aan (en check of er een FG[2] nodig is. Zie:https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/functionaris-gegevensbescherming-fg). De privacycoördinator begeleidt, adviseert bij de invulling van alle privacydocumenten en behandelt de privacyrechten. Tegelijkertijd heeft de coördinator een toezichthoudende rol.
3. Met directie: spreek een budget af! Daarnaast heeft de directie een voorbeeldrol in het uitdragen van/streven naar een privacybewuste organisatie. In een dergelijke organisatie draagt iedereen bij aan de privacy waarborgen en voelt men zich veilig om een riskante situatie of datalek te melden. Formuleer met de directie de uitgangspunten van het privacybeleid. Planning: spreek evaluatiemomenten en jaarlijkse rapportages af.
4. Dashboard: creëer een overzicht van openstaande acties en vooruitgang per afdeling. Richt dit in volgens het organogram van de organisatie. Neem in de planning momenten van implementatie, controle en evaluatie op (PCDA-cyclus).
5. Ga na welke verwerkingen van persoonsgegevens er in de organisatie plaatsvinden. Doe dit door middel van een "nulmeting" of het invullen van het verwerkingenregister.
6. Opstellen privacybeleid intern, voor de eigen organisatie. Dit beleid bevat ook het datalekprotocol en datalekregister.
7. Opstellen van een privacy policy voor de website in begrijpelijke heldere taal.
8. Zorg ervoor dat technische en organisatorische beveiligingsmaatregelen op orde zijn / getroffen worden.
9. In de organisatie: maak een planning voor privacybewustwording en betrokkenheid. Zorg voor goede training (*e-learning*), en organiseer ook regelmatig opfrismomenten. Maak privacy een terugkerend onderwerp in zowel management- als teamoverleg.
10. Waarborgen privacyrechten betrokkenen: stel een protocol op hoe om te gaan met de uitoefening van privacyrechten (inzage, portabiliteit, vernietiging).
11. Check van verwerkingen gegevens kinderen (toestemming)
12. Alle verwerkingen die een hoog risico opleveren voor betrokkenen: maak een risico afweging (DPIA).[3]

[1] De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van de beginselen van de AVG en kan deze aantonen (art. 5 lid 2 AVG)

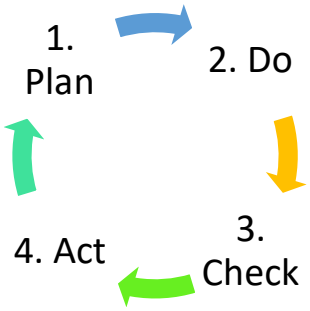
[2] Een Functionaris voor de Gegevensbescherming is verplicht voor publieke- en overheidsinstanties; voor organisaties die vanuit hun kernactiviteiten op grote schaal individuen volgen. Het kan hierbij gaan om bijvoorbeeld profilering van mensen voor het maken van risico-inschattingen, cameratoezicht en monitoring van iemands gezondheid via *wearables*; en voor organisaties die op grote schaal bijzondere persoonsgegevens verwerken en dit een kernactiviteit is.

[3] De AP heeft een lijst opgesteld voor gegevensverwerkingen waarvoor in elk geval een DPIA moet worden gehouden: heimelijk onderzoek; zwarte lijsten; fraudebestrijding; creditscores; financiële situatie; genetische persoonsgegevens; gezondheidsgegevens; samenwerkingsverbanden; (flexibel) cameratoezicht; controle werknemers; locatiegegevens; communicatiegegevens; *internet of things*; profilering; observatie en beïnvloeding van gedrag; biometrische gegevens)

2. Privacycyclus (PDCA)

Om privacy een werkend en levend onderdeel te maken van je organisatie en om aan te kunnen tonen dat je aan je AVG-verplichtingen voldoet (*compliance*), is het handig om volgens een cyclus te werken van **planning** en **controle**. Deze is:

Plan-Do-Check-Act[4]:



1. **Plan:** Vaststellen wat nodig is. Wat zijn de verplichtingen uit de AVG en voldoe ik hier al aan? De organisatie moet in elk geval beschikken over:
   - een privacybeleid & privacy policy,
   - een "privacyverantwoordelijke" die toeziet op de naleving (compliance),
   - een regeling voor datalekken en het uitoefenen van privacyrechten door betrokkenen,
   - ingevuld verwerkingenregister,
   - een beleid voor informatiebeveiliging.

   Eerst moet je weten – observeren - wat de huidige stand van zaken is. Dit kun je het beste doen door middel van een **nulmeting**. *Keep It Simple*: het gaat er hier om een eenvoudige analyse waarmee je het project kunt aansturen.
   Op basis van de nulmeting kun je de actiepunten formuleren waar op dit moment nog niet voldaan is aan de AVG en hoe je dit gaat veranderen.

2. **Do:** Maatregelen treffen. Uitvoeren van de gesignaleerde actiepunten. Implementatie hiervan in de organisatie. Maak een planning waar iedereen zich aan houdt (dashboard).
   Elke afdeling heeft een eigen aanspreekpunt voor de uitvoering van de privacytaken binnen die afdeling.

3. **Check / controle:** Privacy is *work in progress*! Controleer of maatregelen geïmplementeerd zijn en het gewenste effect hebben. Zijn er nieuwe actiepunten bijgekomen? Sommige zaken blijken toch nog niet goed genoeg geregeld of er is een datalek geweest. Al die punten komen dankzij deze controle weer op de actiepuntenlijst. Tip: pak in elk geval met prioriteit de "hete hangijzers" aan, de verwerkingen die hoog risico vormen of waarvan je zelf begrijpt dat de organisatie hierbij een hoog risico loopt en de privacy bij deze verwerkingen goed geregeld moet zijn.

4. **Act**: Ga weer aan de slag met de actiepunten uit de evaluatie/controle. Bijstellen van beleid, procedures en uitvoeringen. Dit is het uitvoeren van punt 3. Doorvoeren van verbeteringen.

[4] Zie ook Wikipedia: "PDCA"

3. Privacybeleid (intern)

Het opstellen van het privacybeleid is een belangrijke stap. Hierin leg je vast hoe de organisatie met persoonsgegevens omgaat, hoe je de beginselen van de AVG invult. Dit moet je schriftelijk vastleggen zodat je ook aan je verantwoordingsplicht voldoet (compliancy).[5] Uitgangspunt van de AVG is dat je persoonsgegevens op een behoorlijke en transparante wijze verwerkt. Het privacybeleid moet hierin richting en handvatten geven. Hieronder volgt een introductie in de privacybeginselen van de AVG en vervolgens tips hoe je dit kunt verwerken in een privacybeleid voor de organisatie.

Privacybeginselen AVG

Persoonsgegevens moeten[6]:

- Op een rechtmatige, behoorlijke en transparante wijze worden verwerkt (**rechtmatigheid, transparantie**);
- Voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld, en mogen vervolgens niet verder met die doeleinden onverenigbare wijze worden verwerkt (**doelbinding**);
- Toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (**dataminimalisatie**)
- Juist zijn en zo nodig worden geactualiseerd, waarbij alle redelijke maatregelen worden getroffen om onjuiste data te wissen / rectificeren (**juistheid**)
- Zoveel als mogelijk bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren en niet langer dan nodig (**opslagbeperking**)
- Door middel van technische en organisatorische beveiliging op passende wijze beschermd worden tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (**integriteit en vertrouwelijkheid**)

Transparantie: de organisatie is er duidelijk over welke gegevens worden verwerkt en waarom. Dit verwerk je in een duidelijke privacy policy die makkelijk leesbaar is.

Doelbinding: Voor elke verwerking stel je vast voor welk doeleinde je de persoonsgegevens verwerkt. Voorbeelden van doeleinden zijn: relatiebeheer, personeelsmanagement, beveiliging van toegang en goederen, aangaan/uitvoeren overeenkomst, marktonderzoek, marketing, screening personeel. Hierbij geldt het belangrijke beginsel van **doelbinding**. Doelbinding houdt ook in dat je niet meer dan nodig verwerkt (noodzakelijkheidsvereiste) en dat dit in verhouding staat met het te bereiken doel.

Verdere verwerking voor ander doeleinde: Als de organisatie de gegevens wil gebruiken voor een ander doeleinde dan waarvoor de gegevens oorspronkelijk zijn verzameld, is dat alleen toegestaan volgens de AVG zolang dit nog verenigbaar is met de oorspronkelijke doeleinden. De vraag die je daarbij moet stellen is: zou ik als betrokkene zelf redelijkerwijs verwachten dat de organisatie dit ook met mijn gegevens doet?

[5] Art. 5 lid 2 AVG.
[6] Art. 5 AVG.

Archivering, wetenschappelijk en statistisch onderzoek worden in principe beschouwd als toegestane verdere verwerking. Er moet dan wel voldaan zijn aan nadere waarborgen van pseudonimisering of anonimisering (zie H.6 Persoonsgegevens).

Direct marketing: aan eigen klanten mag dit op basis van gerechtvaardigd belang, voor anderen is toestemming vereist. De betrokkene mag altijd bezwaar maken tegen direct marketing, ongeacht of de gegevens gebruikt worden binnen het oorspronkelijke doeleinde danwel verdere verwerking. Dit recht van bezwaar moet duidelijk en los van de andere informatie vermeld worden (zie H.13).

Rechtmatigheid: de verwerking moet altijd **rechtmatig** zijn, dus een toegestane grondslag hebben volgens de AVG. Dit kan (o.a.) zijn: toestemming van betrokkene; uitvoering van de overeenkomst; voldoen aan een wettelijke verplichting; maar ook gerechtvaardigd belang (zie voor rechtmatigheid, H. 8).

Beschrijf ook hoe de organisatie de eisen van dataminimalisatie, datakwaliteit en toegankelijkheid toepast in de bedrijfsprocessen:

Dataminimalisatie betekent: niet meer gegevens verwerken dan nodig voor de specifieke verwerking, en data verwijderen zodra je deze niet meer nodig hebt. Hiervoor dien je per verwerking de bewaartermijn vast te stellen.

Datakwaliteit betekent: niet met verouderde data werken, controle van nieuw ontvangen data, periodieke controle van de juistheid van data (in overleg met betrokkenen) en het (automatisch) verwijderen van oude data na verloop van de bewaartermijn. Bepaal per verwerking welke bewaartermijn er geldt zodat deze ook niet langer dan nodig bewaard worden[7].

Privacy by default: software producenten zijn verplicht om in de instellingen een meest privacy vriendelijke optie aan te bieden. Vink deze dus bewust aan in alle software waarmee de organisatie werkt.[8]

Toegankelijkheid: denk na over een uniform systeem of structuur, waarmee data worden opgeslagen. Op die manier kunnen persoonsgegevens ook gemakkelijk worden teruggevonden, bijvoorbeeld wanneer een betrokkene een verzoek doet (uitoefening van privacyrechten) of gegevens gearchiveerd/vernietigd/overgedragen moeten worden.

Welke **organisatorische beveiligingsmaatregelen** tref je? Dit gaat dus over zaken als wachtwoorden, geen rondslingerende stukken en je laptop niet onbeheerd achterlaten. Er zijn simpele maar effectieve beveiligingsmethodes als werken via VPN, tweefactor authentificatie bij gebruik van software.

De effectiviteit van beveiligingsmaatregelen staat of valt echter met de privacy *awareness* binnen de organisatie: begrijpen de mensen het belang, zijn zij gemotiveerd en kunnen zij op de juiste wijze omgaan met data en de systemen? Een goede voorlichting en regelmatige aandacht voor dit onderwerp zijn net zo essentieel als de maatregelen zelf.

Ga met ICT na of de **technische beveiligingsmaatregelen**, aan de actuele eisen voldoen. Denk hierbij aan actuele beveiligingsstandaarden, autorisatie afspraken, beveiliging van toegang, bijhouden van toegang (*logging*), tijdig uitvoeren van updates. Een adequaat backupsysteem,

[7] Zie H. 15 (bewaartermijnen).
[8] Art. 25 AVG: gegevensbescherming door ontwerp en door standaardinstellingen.

versleuteling van data, mail, harde schijf. Zie H.10 voor meer informatie over beveiligingsmaatregelen.

Omgang met privacyrechten: hierin leg je vast hoe je omgaat met een privacyverzoek zoals het recht op inzage, dataportabiliteit, correctie, verwijdering ("recht op vergetelheid"), bezwaar, beperking. Let op, sommige informatie kan niet verwijderd worden vanwege wettelijke voorschriften (zoals het bewaren van financiële gegevens voor de fiscus). Zie voor een overzicht:

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/rechten-van-betrokkenen

Opstellen privacybeleid organisatie

In het privacybeleid dienen de hierboven beschreven privacybeginselen te worden uitgewerkt. Daarbij heb je als organisatie een keuze hóe je deze invult en wat de speerpunten zijn. Zolang je dit maar goed kunt motiveren. Het opstellen van het privacybeleid vraagt dus om een goed doordachte visie op hoe de organisatie met privacy wil omgaan. Deze discussie kan ook ethische aspecten hebben. In elk geval kun je hierbij uiteraard de kernwaarden van de organisatie betrekken. Daarnaast kun je je afvragen of het respecteren van privacy niet een kernwaarde op zichzelf is, of moet worden binnen de organisatie?

Een belangrijke privacywaarde is bijvoorbeeld *privacy by design*[9]. Dit houdt in dat je vanaf het begin rekening houdt met privacy, in de werkwijzen, processen en het inbouwen van software. Ook kun je nadenken over bepaalde grenzen waar je als organisatie een duidelijk signaal over wil geven, zowel intern als extern. Dit kan bijvoorbeeld inhouden dat jullie afspreken om in principe geen gegevens aan derden te verstrekken die geen leverancier zijn (tenzij op basis van een wettelijke plicht), en niet met techbedrijven als Facebook e.d. te werken. Zie hierover ook: H.13 (online marketing) en H.19 (uitwisselen met derden/buiten de EU).

Zie voor inspiratie in deze richting bijvoorbeeld ook:

- https://publicspaces.net/2020/08/18/two-years-of-fighting-for-digital-ethics/
- https://publicspaces.net/2021/12/24/cookies-bij-de-voordeur-technologie-in-de-fysieke-publieke-ruimte/
- https://publicspaces.net/2021/12/14/de-digitale-spoelkeuken-van-start/

[9] Art. 25 AVG.

Twee voorbeelden

Dataminimalisatie
Kernwaarde: mensen moeten zich bij de organisatie vrij en veilig voelen.
Wat betekent dit voor camerabewaking, *wifitracking*? Dataminimalisatie is een belangrijk beginsel in privacy. Dit betekent dat je zo min mogelijk data verwerkt.

Zelf de controle
Kernwaarde: wij willen ons publiek inspireren en ook via website, nieuwsbrieven en online marketing benaderen, terwijl de persoonlijke levenssfeer gewaarborgd blijft. Wellicht betekent dit dat je de betrokkenen zelf op transparante wijze de controle geeft over welke informatie zij met jouw organisatie willen delen, in plaats van "ongemerkt" een profiel over ze op te bouwen met behulp van big data, (tracking) cookies en ze te "targeten" via third party cookies (zie H. 11-13).

Het thema "controle" over eigen data zal steeds groter worden en kan ook een kernwaarde zijn: geef je relaties de keuze welke informatie jouw organisatie over hen verzamelt en geef ze ook de mogelijkheid dit aan te passen wanneer zij willen. Dit kan tot meer wederzijds vertrouwen leiden. Dit kan echter alleen maar als de beveiliging ook goed op orde is.

-> Dus een privacywaarde in het privacybeleid kan ook zijn: het beschermen van data met de best passende (cyber) beveiliging.

In het plan zul je ook voor de afdelingen **concrete grenzen** moeten aangeven van wat wel en niet kan. Van welke bezoekers verzamel je data? Welke data? Ook persoonlijke voorkeuren? Maak je een profiel van elke bezoeker? Koppel je dit aan een postcode? Hebben jullie daar nog wel een wettelijke grondslag voor? Hoe lang bewaar je gegevens na het kopen van een ticket of product; een, twee of vijf jaar? Koppel je dit aan de gegevens die de cookies op de website verzamelen? Gebruik je de gegevens voor social media als Instagram en Facebook? Je bent dan inmiddels gegevens aan het hergebruiken; is dit nog altijd te verenigen met het oorspronkelijke doeleinde van de verwerking? Ben je hierover transparant in de privacy policy? Worden de data door leveranciers/verwerkers buiten de EU gebracht en is sprake van een passend beschermingsniveau?

Deze handleiding geeft je hierop niet de antwoorden, maar uit de volgende hoofdstukken blijkt wel hoe je al deze vraagstukken moet doorlopen, namelijk telkens met de kritische vraag naar de beginselen van behoorlijke (rechtmatige) en transparante (ben je er duidelijk over c.q. vraag je toestemming) verwerking.

Ook is dit het moment om na te denken in hoeverre de organisatie gegevens van kinderen moet verwerken en zo ja hoe dit in het bijzonder geborgd kan worden. Kinderen zijn kwetsbaar en zich niet bewust van de risico's. Eigenlijk wil je als dit kan, zoveel mogelijk wegblijven van het verwerken van deze gegevens, tenzij het noodzakelijk is voor de uitvoering van de (kern)activiteiten van de organisatie. In dat geval zal voldaan moeten zijn aan bijzondere waarborgen.

Awareness: tenslotte, maar heel belangrijk: de organisatie kan de bewuste keuze maken om de eigen medewerkers goed op te leiden in privacy *awareness* en informatiebeveiligingsbeleid. De sleutel tot succes is of de medewerkers de basisbeginselen begrijpen en dit in de praktijk brengen. Ook dit kan een privacywaarde zijn: wij trainen en ontwikkelen onze medewerkers op om zorgvuldige wijze om te gaan met de privacy van ons publiek.

Checklist privacybeleid

- welke waarden?
- op hoofdlijnen, welke verwerkingen?
- voor welke doeleinden (doelbinding)?
- in hoeverre wil je binnen de organisatie data hergebruiken, benoemen van afgeleid doeleinde en afgrenzen van gebruik?
- Rechtmatige verwerking?
- hoe pas je eisen van datakwaliteit en dataminimimalisatie toe?
- welke bewaartermijnen gelden er voor welke gegevens?
- welke technologische en organisatorische veiligheidsmaatregelen heeft de organisatie getroffen?
- hoe ga je om met rechten van betrokkenen (informeren, inzage)?

4. Privacy policy

De privacy policy is niet hetzelfde als het privacyplan. Volgens de AVG heb je een wettelijke informatieplicht om betrokkenen te informeren wat je precies aan gegevens verwerkt, voor welke doeleinden, voor hoelang je deze bewaart, enz.[10] De AVG vraagt hier om een prettig leesbare samenvatting, bestemd voor je klanten/bezoekers/toekomstig medewerkers. De logische keuze is om deze op je website te publiceren. Het is dus handig om dit in begrijpelijke, heldere taal te beschrijven. Daarbij zullen bijvoorbeeld de volgende onderwerpen worden behandeld:

- Hoe en op welke wijze respecteert en waarborgt de organisatie uw privacy?
- welke gegevens verwerken wij bij de volgende processen (bijvoorbeeld):
- bezoek website (cookies)
- online aankopen (tickets, merchandise)
- een account aanmaken
- uitwisseling van welke gegevens met derden als de ticketverkoop via hen verloopt
- beveiligingscamera's
- Donateur worden of andere vorm van gift, abonnement
- nieuwsbrieven en andere communicatie over actualiteiten en events
- sollicitatie
- bewaartermijn van gegevens
- rechten van betrokkenen (inzage, correctie, dataportabiliteit, verwijdering)
- contactgegevens privacyverantwoordelijke / klachtrecht bij Autoriteit Persoonsgegevens

Over alle data die je nodig hebt, maar ook over verdere verwerkingen hiermee voor marketing of onderzoeksdoeleinden, moet je volledig **transparant** zijn: je moet aangeven dat je deze verwerkt, voor welk doeleinde en welk verder doeleinde. Als je bijvoorbeeld toestemming nodig hebt voor een verwerking, bijvoorbeeld van biometrische gegevens, dan zul je daarbij ook expliciete toestemming moeten vragen voor de verdere verwerking. Bijvoorbeeld: iemand verleent toestemming voor DNA-onderzoek om meer te weten te komen over afkomst, voorouders, familie. Als het bedrijf verder (eigen) onderzoek wil doen met jouw DNA zal het daarvoor expliciete toestemming moeten vragen.

Als bepaalde data niet bij jouw organisatie binnenkomen, maar je hier wel over wil beschikken in verband met relatiebeheer, dan kan onderzocht worden of er wellicht sprake is van een gezamenlijke verwerkingsverantwoordelijkheid (zie H.17).

Als de andere partij de verwerkingsverantwoordelijke is en jouw organisatie de "verwerker" dan moet je afspraken maken met deze derden (zoals de ticketing, theater/bioscopen) over de uitwisseling van jouw bezoekersdata en over de informatie aan de betrokkenen voor deze uitwisseling. Voor deze situatie gelden extra eisen en waarborgen. Ook is het belangrijk dat beide organisaties hier volledig transparant over zijn richting de bezoeker en hier verantwoording over afleggen in de privacy policy.[11]

[10] Art. 12 AVG.
[11] Zie art. 14 AVG.

5. Persoonsgegevens

Alles in de AVG draait om de bescherming van persoonsgegevens. Wat is een persoonsgegeven? Dit is een ruimer begrip dan misschien gedacht, want het gaat niet alleen om rechtstreekse informatie over een persoon, maar ook om informatie die te herleiden is naar een persoon; *identificerende* gegevens. De definitie van een persoonsgegeven volgens de AVG[12] is*:*

"Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de "betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentifieeerd, met name aan de hand van een idenfiicator als een naam, identificatienummer, locatiegegevens, online identificator, of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of scoiale identeit van die natuurlijke persoon."

Dus zijn persoonsgegevens niet alleen:

A. alle informatie over een geïdentificeerde persoon
B. maar ook alle informatie over een identificeerbare persoon

Bij **A.** kun je aan de logische gegevens denken als naam, e-mailadres, adres, BSN, nummer identiteitskaart/paspoort.

Bij **B.** gaat het om (indirect) identificerende gegevens. Zonder de naam van de betrokkene kan de informatie, door combinatie met andere gegevens, toch worden herleid tot een persoon. Denk hierbij aan IP-adres, kenteken, geboortedatum, locatiegegevens, postcode, een online identificator, maar ook stem, DNA-profiel, vingeradruk of "*een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psyschische, economische of culturele of sociale identiteit van die natuurlijke persoon.*" Bij dit laatste kun je dus denken aan inkomen of cultureel profiel.

Bijzondere/speciale persoonsgegevens: deze gegevens mag je niet verwerken. Hiervoor geldt een verwerkingsverbod tenzij de persoon **uitdrukkelijke toestemming** heeft gegeven, of er is een noodzaak of wettelijke plicht (art. 9 lid 2 sub a t/m j AVG). Dit zijn bijvoorbeeld gegevens over:

- Ras of etnische afkomst. Een foto is dat niet per se, hieruit blijkt op zich wel iemands afkomst. Maar het hangt af van de context van de verwerking of het een biometrisch gegeven is;
- Politieke opvattingen;
- Religieuze of levensbeschouwelijke overtuigingen;
- Lidmaatschap van een vakbond;
- Genetische gegevens (DNA, RNA, of een analyse van andere elementen waarmee soortgelijke informatie kan worden verkregen);
- Biometrische gegevens (Gegevens die het resultaat zijn van een technische verwerking m.b.t. fysieke, fysiologische of gedragsgerelateerde kenmerken waarmee iemand eenduidig kan worden geïdentificeerd, zoals bijvoorbeeld een vingerafdruk of een irisscan. Een herkenbare foto kan een biometrisch gegeven zijn als de techniek van gezichtsherkenning wordt ingezet);
- Gezondheidsgegevens (gegevens over de fysieke of mentale gezondheid van een persoon);

[12] Art. 4 lid 1 AVG.

- Seksueel gedrag of geaardheid;
- Gegevens over een kind dat jonger is dan 16 jaar: verwerking is alleen rechtmatig met toestemming van de ouders. Kinderen worden specifiek beschermd tegen marketing en *profiling* (het opstellen van gebruikers / persoonlijkheidsprofielen) en het verzamelen van gegevens van kinderen van rechtstreeks aan kinderen verstrekte diensten (geldige toestemming pas vanaf 16 jaar oud)[13];
- Strafrechtelijke gegevens zijn volgens de AVG geen bijzondere gegevens, maar mogen alleen worden verwerkt onder specifieke voorwaarden. Dit kan relevant zijn voor de werkgever (VOG, en wat als een medewerker veroordeeld is voor een strafbaar feit), en bij de verwerking op een "zwarte lijst" bijvoorbeeld van frauderende medewerkers, mensen die overlast veroorzaken of winkeldiefstallen plegen. Een interne zwarte lijst moet aan bepaalde voorwaarden voldoen voordat deze is toegestaan. Een externe zwarte lijst mag niet zonder vergunning van de AP. Let op, de AP kan voor een "illegale" zwarte lijst, zware boetes opleggen. Een recent voorbeeld is de Belastingdienst in de toeslagenaffaire. Zie voor beide onderwerpen verder de website van de AP:

  https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/zwarte-lijst

Beveiliging perssonsgegevens

Persoonsgegevens moeten op een passend beveiligingsniveau worden beveiligd. Beveiligingsmaatregelen zijn: **pseudonimisering en versleuteling[14].**

Versleuteling: kun je doen door persoonsgegevens in een versleutelde bijlage te verzenden (pdf, en/of beveiligd met een wachtwoord), beveiliging van web en mailverkeer, versleutelde verbinding. Zie de website van het Nationaal Cyber Security Center:

https://www.ncsc.nl/onderwerpen/verbindingsbeveiliging

Pseudonimisering is een goede beveiligingsmaatregel in het algemeen, en in het bijzonder van datasets waarvan je de privacy zo goed mogelijk wil waarborgen. Bijvoorbeeld als je met profielen zou willen werken, vraagt de AVG om extra technische maatregelen om nog zo min mogelijk met herleidbare data te werken. Pseudonimiseren betekent het verwijderen van directe identificatoren als naam, IP-adres of geboortedatum. Alleen met een sleutel kan de rest van de gegevens worden herleid tot de betrokken persoon. Belangrijk is hierbij wel dat de sleutel (of de "aanvullende gegevens") apart en beveiligd wordt bewaard.

Een andere mogelijkheid is "**hashen**"; het toepassen van een wiskundige bewerking die informatie (bijvoorbeeld een mac-adres) omzet in een hashwaarde die altijd even lang is. Zie voor een toelichting, de website van de AP:

https://autoriteitpersoonsgegevens.nl/nl/nieuws/techblogpost-praktische-problemen-bij-het-afknippen-van-hashes

Let op: het is een misverstand dat gepseudonimiseerde gegevens anoniem zijn. Dat is niet het geval: gespeudonimiseerde of gehashte gegevens kunnen in combinatie met andere gegevens (of met gebruik van de sleutel) nog altijd worden herleid naar een individu. De AVG is dan ook nog altijd van

[13] Art. 8 AVG.
[14] Art. 32 lid 1 sub a AVG.

toepassing. Het rechtvaardigt mogelijk wel eerder een verwerking in het gerechtvaardigde belang van de organisatie.

Anonieme gegevens zijn zodanig veranderd dat deze niet meer herleidbaar zijn tot een persoon. Om dit te bereiken, moeten alle identificerende gegevens (die herleidbaar zijn tot een persoon) onomkeerbaar worden verwijderd. Ook daarna moet identificatie niet op andere wijze meer mogelijk zijn met behulp van bijkomende of nieuwe gegevens of technieken.

Hoe anonimiseren?

Om een dataset te anonimiseren worden vaak verschillende technieken gecombineerd:

Markeren: het weglakken van een persoonsgegeven als geboortedatum.

Generalisatie: unieke gegevens vervangen met hetzelfde gegeven voor iedereen. Bijvoorbeeld: iedereen dezelfde naam geven. Ook: gegevens van uniek veranderen in iets breders, groters (bijvoorbeeld: in plaats van een woonplaats -> regio; in plaats van een postcode -> letters weglaten van de postcode; in plaats van een geboortedatum -> geboortejaar).

Randomisatie: het "random" (willekeurig) verwisselen binnen een dataset of toevoegen of wissen van bepaalde gegevens. Dit kan door bijvoorbeeld "ruis" toe te voegen. Zie voor meer informatie: https://fgsupport.nl/wat-is-anonimisering

Als je organisatie gegevens wil gebruiken voor wetenschappelijk, statistisch of analytisch onderzoek, dan is anonimiseren een aan te raden stap. De AVG is strikt genomen niet meer van toepassing op anonieme gegevens. Het anonimiseren van gegevens is echter wel een "verwerking" waarvoor je dus vooraf toestemming of een andere gerechtvaardigde verwerkingsgrondslag moet hebben. Zie voor statistisch onderzoek verder H.11.

Let op: de techniek van o.a. "big data" om anonieme gegevens toch weer te herleiden naar een persoon, is al zodanig ontwikkeld dat je eigenlijk nooit echt meer kan worden gesproken van "anonieme data". Wees je hiervan dus bewust en kies er waar mogelijk voor om geen anonieme data uit handen te geven aan derden waarmee geen verwerkersovereenkomst bestaat.

Voor verdiepende informatie: er is een handleiding uit 2014 (van de voorloper van de EPDP) over anonimiseringstechnieken, waar de meeste privacy toezichthouders nog steeds naar verwijzen:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

6. Verwerkingsregister

Het bijhouden van een register is in principe verplicht voor elke organisatie die niet op incidentele basis gegevens verwerkt.[15] Daarnaast draagt het bij aan het verkrijgen van inzicht en controle: het register is een perfect meetinstrument of de privacywaarborgen binnen de organisatie op orde zijn en om te monitoren dat hieraan gewerkt wordt (*compliance*).

Het verwerkingsregister moet per afdeling worden ingevuld. Je kunt de eerste keer invullen van het verwerkingsregister ook als nulmeting beschouwen (in de PDCA-cyclus).

In principe is voor alle bedrijfsprocessen de organisatie de “verwerkingsverantwoordelijke”. Zie voor uitleg over dit begrip “verantwoordelijke” versus “verwerker” H.17. Het verwerkingsregister begint met de contactgegevens van de verwerkingsverantwoordelijke, te weten de organisatie (naam, vestiging, land) en de contactpersoon: dit kan het afdelingshoofd zijn of de privacycoördinator.

Om dit te kunnen invullen is het erg belangrijk dat je collega’s hierin begeleid worden en enige kennis hebben van privacy. Op die manier kunnen ze er gemakkelijk mee aan de slag. Ook is het belangrijk dat zij gemotiveerd zijn om hier wat van te maken. Voorlichting, training, bevorderen van privacy *awareness* en *commitment* om de organisatie naar een hoger privacyplan te tillen, zijn dus essentieel. Het verwerkingenregister is vormvrij: als bovenstaande onderwerpen maar zijn geadresseerd. Dit kun je bijvoorbeeld bijhouden in een Excelsheet of in Word, bijvoorbeeld per proces een pagina. Er zijn ook tools beschikbaar en natuurlijk kun je ook door een deskundige laten checken of het ingevulde register *compliant* is. Hoe dan ook, beginnen is hier het belangrijkste.

De eerste keer invullen van het register kan erg lastig zijn. Het is verstandig om hier begeleiding en ondersteuning bij aan te bieden door het privacyteam, de privacycoördinator of een externe deskundige. Een andere optie is bijvoorbeeld dat de afdelingshoofden in een privacysessie gezamenlijk het register invullen of hun vragen bespreken.

Het verwerkingenregister vul je in per afdeling, en vervolgens onderverdeeld per proces. Dus bijvoorbeeld voor HR kun je de hele cyclus van solliciteren, indiensttreden, functioneren, ziekte en reïntegratie en uitdiensttreding per proces doorlopen. Zo kun je voor elke afdeling de werkzaamheden in een volgorde, cyclus of structuur op een rijtje zetten.

Per proces / verwerking moet worden nagegaan met welk doeleinde je gegevens verwerkt. Dit mag vrij algemeen zijn. Denk bijvoorbeeld aan relatiebeheer, personeelsmanagement of financiële administratie.

Vervolgens onderzoek je de rechtmatigheid van de verwerking: welke gerechtvaardigde grondslag heeft de organisatie heeft om de bewuste persoonsgegevens te mogen verwerken: toestemming door betrokkene; uitvoering van een overeenkomst; voldoen aan een wettelijke verplichting; noodzakelijk voor de vervulling van een taak van algemeen belang. Het is geen wettelijk vereiste de rechtmatigheid in het register te vermelden (wel in het privacybeleid). Toch kan het verstandig zijn dit te laten invullen zodat er goed over nagedacht wordt (eventueel met behulp van de privacycoordinator)

[15] Art. 5-2, art. 30 AVG.

Van wie worden gegevens verzameld? Dit zijn medewerkers, bezoekers, relaties, leveranciers.

Is het verwerkingenregister helemaal ingevuld? Dan zal het volgend jaar opnieuw geëvalueerd worden en zonodig bijgesteld. Tegen die tijd zijn sommige processen alweer veranderd of bijvoorbeeld uitbesteed, waardoor opnieuw de belangen- en risicoafweging (DPIA) moet plaatsvinden en moet opnieuwworden gekeken naar (o.a.) passende beveiligingsmaatregelen.

Checklist register, per verwerking/proces[16]:

- Naam en contactgegevens verwerkingsverantwoordelijke (de organisatie/ afdelingshoofd en/of privacycoördinator);
- doeleinde(n) van de verwerking (doelbinding) (bijvoorbeeld relatiebeheer, personeelsmanagement, financiële administratie);
- (niet wettelijk verplicht, wel belangrijk vanuit privacybeginselen): grondslag(en) van de verwerking (rechtvaardig gebruik (per proces/verwerking moet worden nagegaan welke grondslag de organisatie heeft om de bewuste persoonsgegevens te mogen verwerken: toestemming door betrokkene; uitvoering van een overeenkomst; voldoen aan een wettelijke verplichting; noodzakelijk voor de vervulling van een taak van algemeen belang;
- de categorie personen van wie je gegevens verwerkt: klanten/bezoekers, werknemers, leveranciers en alle andere contacten;
- welke gegevens verwerk je van hen;
- is sprake van verwerking van bijzondere persoonsgegevens? Zo ja, is er toestemming of een andere rechtvaardigingsgrond?
- of is er sprake van uitwisseling van data aan een derde land of internationale organisatie en zo ja, zijn er dan passende waarborgen getroffen?
- Indien mogelijk, de bewaartermijn waarna de gegevens worden gewist;
- Indien mogelijk, algemene beschrijving van technische en organisatorische beveiligings-maatregelen.

[16] Art. 30 AVG.

7. Doelbinding

Je begint met het (per proces) vaststellen met welk doel je persoonsgegevens verwerkt en welke persoonsgegevens je in dit kader nodig hebt. Persoonsgegevens mogen alleen binnen het vastgestelde doeleinde worden verwerkt en er mogen niet meer gegevens worden verwerkt dan strikt noodzakelijk (doelbinding, dataminimalisatie). Doelbinding houdt in:

"persoonsgegevens mogen alleen worden verwerkt ten behoeve van welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden".

Het is volgens de AVG immers niet toegestaan om persoonsgegevens die voor een bepaald doel zijn verzameld, opeens voor een heel ander doel te gaan verwerken. Dit is de "strikte doelbinding". Het is echter wél toegestaan om de persoonsgegevens later voor een ander doel te gebruiken dan waarvoor ze aanvankelijk zijn verkregen, mits dit niet gebeurt op een wijze die onverenigbaar is met het doel waarvoor de gegevens zijn verzameld - "**verenigbaarheidstoets**":

a) de mate van verwantschap tussen het oorspronkelijke doeleinde en doeleinde(n) van verdere verwerking;
b) de omstandigheden waaronder/context waarbinnen de gegevens zijn verzameld;
c) de redelijke verwachtingen van de betrokkenen op basis van hun verhouding met de organisatie (verwerkingsverantwoordelijke);
d) De aard van de persoonsgegevens;
e) de impact van de verdere verwerking voor de betrokkene;
f) getroffen maatregelen om de impact te beperken (passende waarborgen)

Bij passende waarborgen kun je denken aan versleuteling, pseudonimisering en anonimisering van persoonsgegevens en natuurlijk verdere technische beveiliging van deze data(set).
De betrokkene moet over deze verdere verwerking uiteraard transparant en volledig worden geïnformeerd en moet ook gewezen worden op zijn recht om hier bezwaar tegen te maken.

Om te bepalen of je als organisatie het gerechtvaardigd acht om gegevens verder te verwerken, zul je bovenstaande toets moeten doorlopen. De belangenafweging, van de gerechtvaardigde bedrijfsbelangen versus de belangen van de betrokkene, moet je hierbij *uitschrijven*. Dit zodat je ook kunt verantwoorden dat de privacy afweging heeft plaatsgevonden ("**verantwoordingsplicht**").

8. Rechtmatigheid van de verwerking (grondslagen)

De verwerking van persoonsgegevens is alleen rechtmatig als de organisatie hiervoor over een juridische rechtvaardiging = grondslag beschikt[17]. Het hangt van de verwerking af welke grondslag daarbij past. Soms zal een verwerking meerdere grondslagen hebben: benoem deze dan allemaal. Bepaal ook direct de bewaartermijn zodat - waar mogelijk - al meteen in het proces wordt georganiseerd hoelang de gegevens uiterlijk worden bewaard en vervolgens na verloop daarvan worden vernietigd.

De meest belangrijke **grondslagen** op basis waarvan persoonsgegevens mogen worden verwerkt, zijn[18]:

- **Uitvoering overeenkomst**:

Voor de uitvoering van een contract of dienst heb je een aantal gegevens nodig. Bijvoorbeeld het verkopen van een online ticket: naam, e-mailadres en telefoonnummer. Bijvoorbeeld voor het aangaan/de uitvoering van een arbeidsovereenkomst: gegevens voor in de arbeidsovereenkomst/ salarisadministratie.

De bewaartermijn is gedurende het contract + een x aantal maanden of jaar daarna.

- om **wettelijke verplichtingen** na te komen:

  Een goed voorbeeld hiervan is dat elke organisatie de wettelijke verplichting heeft een administratie bij te houden van crediteuren, debiteuren, voor de BTW en voor een correcte jaarrekening. Voor de fiscus moeten deze gegevens zeven jaar bewaard blijven.

  Een ander voorbeeld is: het is wettelijk verplicht om in de arbeidsovereenkomst persoonsgegevens te verwerken, denk aan de wettelijke verplichting een werknemer te identificeren; aan te melden voor de loonbelasting; de loonadministratie te voeren/ loonstrook te verschaffen; het functioneren te begeleiden en te monitoren; een ziekte- en reïntegratiedossier bij te houden (hiervoor bestaat zelfs een grondslag in de AVG).

  Let op: de wet zal bepaalde minimale gegevens vereisen, maar vaak wil je meer gegevens verzamelen ten behoeve van bijvoorbeeld relatiebeheer of marktonderzoek. Deze verwerkingen moet je dan baseren op een andere grondslag, te weten gerechtvaardigd belang, of je zult toestemming moeten vragen (bijvoorbeeld om gegevens van een sollicitant langer te mogen bewaren).

- **handelen met het oog op een gerechtvaardigd belang van de organisatie, *mits* dit geen ernstige gevolgen heeft voor de fundamentele rechten en vrijheden van de betrokkene.**

Bijvoorbeeld: een organisatie heeft een legitiem belang bij beveiliging van het pand, de daarin bewaarde zaken en haar bezoekers, en kan daartoe bijvoorbeeld een camerasysteem installeren. Ook relatiebeheer, marktonderzoek en het monitoren van bezoekgedrag op de eigen website valt onder gerechtvaardigd belang.

[17] Art 6 AVG: rechtmatigheid van de verwerking.
[18] Dit overzicht is beperkt tot de meest gebruikte grondslagen, zie voor een volledig overzicht: art. 6 AVG.

- **Belangenafweging**: bij het gebruik van deze grondslag zul je altijd een belangenafweging moeten maken waarbij de bedrijfsbelangen worden afgewogen tegen die van de betrokkene. Daarbij neem je mee:
- wat de impact is op de privacy van de betrokkene,
- welke maatregelen je hebt getroffen om die impact te verkleinen, en
- of je de betrokkene de mogelijkheid hebt gegeven om zich af te melden voor deze verwerking (opt-out).

  Als deze belangenafweging negatief uitpakt dan zul je de (expliciete en specifieke) toestemming van de betrokkene moeten vragen om alsnog deze verdere verwerking te kunnen uitvoeren.

Bijvoorbeeld: een museum overweegt de bezoekers van een tentoonstelling te laten volgen met een *beacon* via bluetooth. Het gerechtvaardigde belang van het museum is te monitoren waar het publiek graag naar kijkt en welke paden men loopt (populariteit, effectiviteit van de tentoonstelling en veiligheid). De impact hiervan is groot op de bezoekers, zij worden constant gevolgd. Pas de belangenafweging toe, en neem maatregelen om impact te verkleinen: kondig met een duidelijk bord aan dat via bluetooth gemonitord wordt en adviseer de bluetooth uit te zetten indien men dit niet wil. Sla de gegevens geanonimiseerd op en voor zo kort mogelijke periode.

- **Toestemming** (ondubbelzinnige wilsuiting) van de betrokkene[19]:

  - Deze grondslag moet je gebruiken als er geen contract of wettelijke verplichting voor de verwerking is en je geen gebruik kunt maken van het gerechtvaardigd belang; of als de wet toestemming verlangt (bij de verwerking van bijzondere persoonsgegevens);;
  - De toestemming moet de betrokkene controle geven over het al dan niet verwerken van zijn gegevens;
  - De toestemming moet bovendien **geïnformeerd, specifiek, vrijwillig en ondubbelzinnig zijn** en mag elk moment weer worden **ingetrokken**;
  - Dus als je toestemming vraagt, dan moet je er duidelijk bij vermelden wat je met de gegevens gaat doen, op welke manier en door wie;
  - Als je toestemming hebt voor een bepaalde verwerking, dan moet je dit kunnen aantonen. Dit wordt de **verantwoordingsplicht** genoemd;
  - Om hieraan te kunnen voldoen, moet je een **log** bijhouden zodat de toestemming later te reproduceren is;
  - Als je voor verschillende verwerkingen toestemming vraagt, moet elke verwerking specifiek beschreven zijn en moet je hier afzonderlijk toestemming voor kunnen geven.

Een voorbeeld van toestemming is bijvoorbeeld het verzenden van een nieuwsbrief (direct marketing) aan derden die geen klant of voormalige klant zijn.

- De grondslagen "**handelingen van levensbelang",** en een "**opdracht van openbaar belang"** worden hier volledigheidshalve vermeld maar verder niet besproken in dit naslagwerk.

Zie voor een praktisch overzicht ook:

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stappenplan_verwerken_persoonsgegevens.pdf

[19] Art. 7 AVG, voorwaarden voor toestemming.

9. Technische en organisatorische beveiligingsmaatregelen

Persoonsgegevens moeten goed beschermd zijn tegen verlies, onjuist/ongeautoriseerd gebruik en cybercriminaliteit. Hiertoe moet een passend gegevensbeschermingsbeleid van kracht zijn. Dit beleid waarborgt en toont aan dat persoonsgegevens volgens de AVG worden verwerkt[20].

Het beveiligingsbeleid moet worden opgenomen in de PCDA-cyclus waardoor het periodiek wordt geëvalueerd en zonodig geactualiseerd.

Passende gegevensbescherming:

Afhankelijk van de aard en context van de verwerking, en de te verwachten risico's gelet op de soort persoonsgegevens, moeten passende beschermingsmaatregelen worden getroffen. Deze zijn onder te verdelen in organisatorische- en technische maatregelen. De meeste maatregelen dien je sowieso te treffen. Verdergaande en technische maatregelen moeten worden toegepast; als sprake is van een "hoog risico" verwerking.

Organisatorisch

- *Awareness*, maak medewerkers bewust: geef training en instructies aan personeel. De meeste datalekken komen nogal altijd voort uit onoplettendheid of onwetendheid. Het is belangrijk dat de medewerkers zich verantwoordelijk voelen en concrete tips krijgen over hoe zij kunnen handelen;
- Vastleggen rollen en verantwoordelijkheden voor informatiebeveiliging;
- Informatiebeveiligingsbeleid;
- Leveranciersrelaties (verwerkersovereenkomsten);
- Controle op naleving (control in PCDA-cyclus, audit);
- *Clean desk*-beleid;
- Principe van dataminimalisatie bij alle werkprocessen;
- Geheimhoudingsverplichting door de medewerker tijdens en na afloop arbeidsrelatie;
- Instructie omgang met en opslag van data;
- Instructie thuiswerken (bijvoorbeeld via VPN en nooit op openbaar netwerk surfen / communiceren, "slimme" apparaten die meeluisteren?);
- Datelekprotocol;
- Tijdig afsluiten van accounts/bevoegdheden bij ziekte, schorsing of ontslag;
- Autorisaties voor inzage in documenten/systemen;
- Bewaartermijnen vaststellen;
- Datalekprotocol;
- Datalekregister;
- Oefenen met werkwijze beveiligingsincident.

[20] Art. 32 AVG: beveiliging van de verwerking.

Technische maatregelen

- Bepalen en instellen van de noodzakelijk geachte mate van beveiliging (hiervoor bestaan standaarden zoals ISO 27001);
- Bedrijfsplan continuïteit netwerken, toegang tot persoonsgegevens;
- Werkwijze bij incident zoals *hack* of *ransomware;*
- *Privacy by design, by default* principes toepassen op netwerk, software, gebruik platformen;
- (tijdig) Actualiseren van IT-systemen (levenscyclus);
- Updates software z.s.m. installeren;
- Back-up data: volgens 3-2-1 principe; 3 kopieën, op 2 plekken waarvan 1 offline;
- E-mailcommunicatie beschermd via betrouwbare encryptie;
- Afdwingen van sterke wachtwoorden;
- tweefactor-authenticificatie;
- harde schijf versleutelen;
- beveiliging mobiele apparaten;
- VPN bij thuiswerken;
- Autorisatie beheren en gebruik loggen. Signalering als hier opmerkelijke activiteiten in plaatsvinden;
- Fysieke toegang beveiligen via toegangspasjes, camerasysteem;
- Instellen automatisch verwijderen na aflopen bewaartermijn en voorafgaande notificatie;
- Pseudonimisering/anonimisering/*hashing* van persoonsgegevens (bij hoog risico of “verdere verwerking” op basis van gerechtvaardigd belang);
- Kwetsbaarheden testen systeem.

Zie voor een handig overzicht ook:

https://www.ictrecht.nl/hubfs/Ransomware%20checklist.pdf?utm_referrer=https%3A%2F%2Fwww.ictrecht.nl%2Fsecurity-ransomware

En de tips van de AP:

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/acties-bij-een-datalek?qa=beveiligingsmaatregelen&scrollto=1

Een voorbeeld

400.000 euro boete voor Transavia

De AP heeft op 12 november 2021 een flinke boete uitgedeeld aan Transavia van 400.000 euro. Hun netwerk bleek beveiligd met wel heel erg simpele wachtwoorden. Deze wachtwoorden waren makkelijk te raden (zoiets als "welkom123"). Er was geen twee-factor-authentificatie ingesteld. In 2019 werd het systeem gehackt. Eenmaal binnen kon de hacker de gegevens van 25 miljoen passagiers inzien. De hacker heeft van 800.000 passagiers gegevens gedownload. Transavia verwerkte gegevens als naam, geboortedatum, geslacht, e-mailadres, telefoonnummer en vlucht- en boekingsgegevens, maar van sommige passagiers ook medische gegevens (handicap).

De AP signaleert dat in 2020 het aantal hacks met als doel het bemachtigen van persoonsgegevens explosief is toegenomen. Zolang hackers hier makkelijk mee wegkomen (en sommige landen ondernemen hier geen acties tegen) is dit een lucratief verdienmodel. Een dergelijke hack zal dan dus ook niet alleen tot schade leiden in de vorm van een boete door de AP, maar ook tot potentiële schadeclaims van betrokkenen, en heel belangrijk, reptutatieschade.

De AP geeft ook aan dat door simpele maatregelen als meer-factor-authentificatie veel gevallen van hacking, malware en phishing voorkomen hadden kunnen worden.

Hoe weet je nu of er een passend beveiligingsniveau wordt geboden? Hiervoor is het instrument van risicoafweging:

- welke soort persoonsgegevens (gewone, gevoelige of zelfs bijzondere persoonsgegevens, gegevens van kinderen);
- de aard, het toepassingsgebied, de context en doeleinden van de verwerking;
- gaat de verwerking gepaard met een risico of een hoog risico. Hoog risico voor betrokkenen is bijvoorbeeld dat de verwerking kan leiden tot ernstige materiële of immateriële schade (bijvoorbeeld: discriminatie, identiteitsfraude, financiële verliezen, reputatieschade).

Deze inschatting van mogelijke schade en dreigingen leidt tot beveiligingseisen/maatregelen om dit risico te beperken. Dit wordt ook risicomanagement genoemd: de gepaste maatregelen nemen zodat niet over- of onderbeschermd wordt.

Tegelijkertijd moet de verwerking van persoonsgegevens ook voldoen aan de volgende vereisten: Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV-vereisten)[21].

- **Beschikbaarheid**: gegevens moeten op elk moment toegankelijk zijn/kunnen worden opgevraagd (dus via een goede structuur terug te vinden zijn en via adequate systeem/back-up worden bewaard. Hierover kunnen afspraken worden gemaakt indien de gegevens in de cloud worden bewaard)

[21] Art. 32 lid 1 sub b en c AVG.

- **Integriteit**: correct zijn van data (gecheckt bij ontvangst, periodiek geactualiseerd en na bewaartermijn verwijderd)
- **Vertrouwelijkheid**: alleen geautoriseerden, die ook een geheimhouding hebben getekend, hebben toegang tot gegevens en dit wordt via logging bijgehouden. Dit element ziet ook op beveiliging van vertrouwelijkheid tegen (onopzettelijk/opzettelijk) verlies of inbreuk op de vertrouwelijke gegevens (via *hacking*, *malware*)

Dit leidt tot de volgende risicocategorieën:

Verwerking: ……	Laag	Midden	Hoog
Beschikbaarheid			
Integriteit			
Vertrouwelijkheid			

Afhankelijk van het risicoprofiel zullen passende maatregelen moeten worden getroffen. Neem bijvoorbeeld een psychiatrische instelling. Hier worden bijzondere persoonsgegevens verwerkt. Op alle vlakken van beschikbaarheid (snel kunnen oproepen gegevens), integriteit (juistheid en niet verouderd zijn) en vertrouwelijkheid (de gegevens zijn alleen toegankelijk voor geautoriseerde medewerkers met een geheimhouding) kom je hier op een hoge score. Dit betekent dat ook dat de beveiligingsmaatregelen ook van het hoogste niveau moeten zijn.In dat geval kan mogelijk ook een verplichting bestaan om een DPIA te houden.[22]

- Het kan praktisch zijn om alle beveiligingsmaatregelen inclusief risicomanagement in hetzelfde beleid te regelen.
- Aansluiten bij een gedragscode of branchecode wordt in de AVG aangeraden en bespaart mogelijk een hoop uitzoekwerk.[23] Als er in de branche nog geen gedragscode is, kun je bij de brancheorganisatie informeren of zij deze kunnen opstellen.
- Zie voor meer informatie, bijvoorbeeld de BIO van de Rijksoverheid waarin één standaardbeleid is voor informatiebeveiligingsbeleid: https://www.bio-overheid.nl/
- Ook Wikipedia heeft een informatieve pagina over informatiebeveiliging: https://nl.wikipedia.org/wiki/Informatiebeveiliging

[22] Art. 35, Gegevensbeschermingseffectbeoordeling.
[23] Art. 40 AVG: Gedragscodes.

Een voorbeeld

Boete wegens o.a. gebrekkige informatie en beveiligingsbeleid

Het psychotherapiecentrum Vastaamo in Finland heeft in september 2020 bij de nationale toezichthouder ("de ombudsman") een melding gemaakt van een aanval op haar patiëntendossier. Naar aanleiding hiervan heeft de Ombudsman een onderzoek gestart naar de rechtmatigheid van de activiteiten van Vastaamo. Daaruit waren de bevindingen dat Vastaamo haar taken verwaarloosde met betrekking tot de veilige verwerking van persoonsgegevens en het melden van een inbreuk in verband met persoonsgegevens.

Op basis van een technisch onderzoek bleek dat Vastaamo al veel eerder moet hebben geweten dat de patiëntgegevens waren verdwenen en dat deze mogelijk al in maart 2020 in het bezit van een externe aanvaller zouden zijn beland. Vastaamo had de inbreuk destijds onverwijld moeten melden aan zowel de toezichthoudende autoriteit, als haar klanten.

De persoonsgegevens waren niet naar behoren beschermd tegen ongeoorloofde en illegale verwerking of onopzettelijke verdwijning, en Vastaamo had geen basismaatregelen genomen om de veilige verwerking van persoonsgegevens te waarborgen. Door onvoldoende documentatie kon Vastaamo evenmin aantonen dat zij aan de gestelde veiligheidseisen zou hebben voldaan.

Vastaamo kreeg een boete van 608.000 euro opgelegd. Daarbij achtte men de daden van nalatigheid zeer ernstig en het handelen van Vastaamo bij het nalaten van de meldingsplicht opzettelijk. Bovendien waren de overtredingen langdurig.

10. Statistisch onderzoek

Culturele organisaties zullen voor bijvoorbeeld hun subsidiegevers, maar ook voor eigen informatie statistische gegevens willen verzamelen van hun bezoekers, de kopers van hun producten en/of de afnemers van hun diensten.

Dergelijk onderzoek is toegestaan, mits van **passende waarborgen** volgens de AVG voorzien[24]:

Er dienen technische en organisatorische maatregelen te worden getroffen om dataminimalisatie te realiseren. Een dergelijke maatregel kan **pseudonimisering** zijn, maar waar mogelijk **anonimisering** (zie H. 6 "Persoonsgegevens").

Het doel van statistisch onderzoek moet zijn de verwerking van geaggegreerde gegevens. Het resultaat hiervan wordt niet gebruikt als ondersteunend materiaal voor maatregelen of beslissingen die een natuurlijke persoon betreffen.

➔ Met de statistiek mag je dus niet weer gericht personen gaan benaderen voor doeleinden als marketing. In dat geval ben je niet meer bezig binnen het doel "statistisch onderzoek".

Een voorbeeld van statistisch onderzoek: van een dataset worden naam, adres, IBAN verwijderd (dataminimalisatie) en van de postcode de letters verwijderd – (pseudonimisering). Hiermee wordt een statististiek verkregen van de herkomst van de bezoekers.

Wifi/bluetooth tracking

Veel winkels vinden het interessant om te meten hoe lang bezoekers zich in een ruimte bevinden, omdat dit waardevolle informatie biedt voor de inrichting van de ruimte en inzicht geeft in welke producten of objecten interessant worden gevonden. Een instrument dat zij daarbij inzetten is *wifi/ bluetooth tracking*:

Tracking werkt als volgt. Een mobiele telefoon zendt voortdurend signalen uit waarmee de aanwezigheid kenbaar wordt gemaakt. Deze signalen bevatten een uniek identificatiekenmerk, het "Media Access Control-adres" (hierna: mac-adres). Mac-adressen zijn de unieke nummers die door de fabrikant zijn vastgelegd in de hardware van apparatuur, zoals op geheugenchips en/of netwerkkaarten in laptops en telefoons. Omdat elk mobiel apparaat een uniek bluetooth- en een uniek wifi-mac-adres heeft, kunnen apparaten op specifieke locaties herkend worden.

Rechtmatigheid?

Let op: het verzamelen van gegevens via tracking kan niet plaatsvinden op basis van de uitzondering van "statistisch doeleinde". Daar is deze zeer beperkte uitzondering niet voor bedoeld.
De grondslag van toestemming is realistisch niet haalbaar, want hoe kun je nu iedereen bij de ingang om ondubbelzinnige geïnformeerde toestemming vragen?
Hiervoor geldt dan ook met name het kader van de grondslag "gerechtvaardigd belang" met bijbehorende belangenafweging.[25]

Het is belangrijk om te weten dat de AP hierin een vrij strenge benadering hanteert waarbij in feite alleen nog is toegestaan om op basis van gerechtvaardigd belang de bewegingen te monitoren ten behoeve van fysieke veiligheid van personen en de beveiliging van eigendommen.

[24] Art. 5 lid 1 sub e) en f).
[25] Art. 6 lid 4 AVG.

Wanneer het doeleinde is om het succes van een bepaalde tentoonstelling te meten, dan valt dit daar dus niet zomaar binnen. Het monitoren of er niet teveel mensen in één ruimte verkeren i.v.m. brandveiligheid valt hier wél binnen.

- Er moet dan nog wél voldaan zijn aan de noodzakelijkheidstoets (is het echt nodig om op deze wijze gegevens te verzamelen), en;
- de belangenafweging tussen het gerechtvaardigde belang van de verwerkingsverantwoordelijke versus de belangen, grondrechten en fundamentele vrijheden van de betrokkene (zeker als dit een kind is) bij bescherming van persoonsgegevens;
- tenslotte moet de organisatie technische- en organisatorische maatregelen treffen om de privacy zoveel mogelijk te beschermen, bijvoorbeeld:

  - anonimisering direct bij de sensor, dus het verwijderen van het mac-nummer en toevoegen van een ander *random* nummer;
  - dataminimalisatie: beperken van de metingen tot specifieke tijden en locaties (in plaats van 24 uur per dag en 7 dagen per week);
  - per meetlocatie *hashen* van gegevens zodat de mensen niet over meerdere ruimtes en tijd kunnen worden gevolgd;
  - opt-out aanbieden: bezoekers de mogelijkheid bieden om zich af te melden voor wifi/*bluetooth tracking* waarmee zij zich aan de metingen kunnen onttrekken. De opt-out mogelijkheid moet duidelijk kenbaar zijn!
  - Informatieverplichting: Als organisatie blijf je altijd verplicht om heel duidelijk te maken dat persoonsgegevens worden verwerkt via *wifitracking*. Zie voor informatierecht: H.14.

11. Profilering

Wat is profileren? Dat is: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij persoonlijke aspecten van een persoon worden geëvalueerd, met de bedoeling om zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren, of te voorspellen (art. 4-4 AVG).

Het gaat dus om de *geautomatiseerde besluitvorming* op basis van deze profielen. De AVG bevat een verbod om op basis van geautomatiseerde besluitvorming / profiling besluiten te nemen die rechtsgevolg hebben of anderszins de betrokkene in aanmerkelijke mate treffen.[26] Denk hierbij aan het toekennen van een kredietscore, het afwijzen van een lening, het afwijzen van een sollicitatie.

Het verbod geldt niet indien:

a. dit nodig is voor de uitvoering van een overeenkomst, of
b. de betrokkene uitdrukkelijke toestemming heeft verleend, en
c. betrokkene hierover vooraf actief is geïnformeerd. Daarbij dient de onderliggende logica, het belang en de verwachte gevolgen van die verwerking voor de betrokkene worden vermeld (aanvullende informatieverplichting),
d. Daarnaast dient betrokkene geïnformeerd te zijn over alle privacyrechten (recht om toestemming te allen tijde in te trekken, informatie over bewaartermijn, recht van bezwaar, wissing, rectificatie, inzage en klacht bij AP).

Als het gaat om gegevens die van een ander zijn verkregen, dan gelden weer verdergaande waarborgen. Zowel de verstrekker als de ontvanger moeten de betrokkene hierover informeren en alle relevante informatie verstrekken zoals hierboven bij c. vermeld. Dat doet hij op het moment:

- binnen redelijke termijn, maar uiterlijk binnen een maand na het verkrijgen van de gegevens;
- als de gegevens zullen worden gebruikt voor communicatie met betrokkene, het eerste contact;
- als wordt overwogen om de gegevens aan een andere ontvanger te verstrekken, uiterlijk het tijdstip van overdracht.

- Mocht de organisatie overwegen om met profielen op basis van niet zelf verkregen data te gaan werken dan is het raadzaam dit hele proces zowel op het gebied van informatieveiligheid als privacy *compliance* te laten toetsen, zodat dit verantwoord en in lijn met de AVG kan gebeuren: denk hierbij aan de extra eisen (risico-belangenafweging (dpia)), verwerkingsgrondslag (toestemming bij niet-klanten?), doelbinding, integriteit data (BVI), beveiligingsmaatregelen waaronder pseudonimisering/anonimisering/*hashing*.

Zie voor online marketing (met behulp van “profiling”) het volgende Hoofdstuk 12.

[26] Art. 4 lid 4 AVG, art. 22 AVG.

12. Online marketing

In een toenemende digitale wereld is er ook steeds meer vraag naar de online marketing activiteiten. Dat maakt de verantwoordelijkheid er juist niet minder om. Met de gegevens van je klanten wil je zuinig omspringen.

Het belangrijkste is hier, om (naast een check van de doelbinding en rechtmatigheid) na te denken met welke leveranciers (tools, social media) je werkt en of deze objectief (volgens de eisen van de AVG) en subjectief (volgens de privacywaarden van de organisatie) op een verantwoorde wijze de data zullen verwerken. Deze grenzen zijn af te leiden uit het privacybeleid van de organisatie, maar per tool of social media moet daarover opnieuw bewust nagedacht worden en moet dit ook worden vastgelegd in het privacybeleid, verwerkingenregister en verwerkersovereenkomst. Op die manier zijn ook de rollen, verantwoordelijkheden en grenzen voor iedereen duidelijk.

Let op: elke tool zal in de instellingen al bepaalde privacywaarborgen aanbieden. Het is dan ook de verantwoordelijkheid van de organisatie (in overleg met ICT) om hier standaard (*default*) de meest privacyvriendelijke instellingen aan te zetten[27]. Ook moet hier meteen goed nagedacht worden over dataminimalisatie. Welke gegevens kunnen worden weggelaten terwijl nog steeds de verwerking kan plaatsvinden?

Ook moet worden onderzocht of de gegevens bij de verwerker wel in de EU blijven of dat deze worden uitgewisseld met derde landen. In dit laatste geval moet er kritisch worden getoest of er passende waarborgen zijn getroffen.

Op dit moment geldt de E-Privacy Richtlijn. De regels hiervan zijn geïmplementeerd in de Telecommunicatiewet. Uitgangspunten zijn: eerbiediging persoonlijke levenssfeer (privacy); vertrouwelijke communicatie, voorschriften m.b.t. cookies, een verbod om overlast te veroorzaken met ongevraagde commerciële elektronische berichten (**spamverbod**).

De opvolger hiervan, de E-Privacy Verordening (ePV) wordt voorbereid in Europa, maar is nog niet in werking. Deze zal net als de AVG rechtstreekse werking hebben. Deze verordening betreft ook actuele vormen van elektronische communicatie. Bijvoorbeeld IOT (internet der dingen), internet-telefonie (zoals Skype) en de diensten van internetproviders - niet alleen persoonlijke gegevens, ook metadata, verwerkt als "big data". Ook bevat deze verplichtingen inzake vernietigen van gegevens na verzending en een herziening van de cookieregeling, met onderscheid tussen technisch-noodzakelijke en andere cookies.

Spamverbod

Direct mailing (via sms, app, mail, maar ook directe berichten op social netwerksites als Facebook) is alleen toegestaan als je toestemming hebt of als het een bestaande/voormalige klant betreft:

- Aan derden (niet (voormalige) klanten): Op basis van toestemming: de organisatie moet kunnen aantonen dat je inderdaad over toestemming beschikt. Deze moet je vijf jaar bewaren;
- Aan eigen klanten mag dit binnen de grondslag van het gerechtvaardigde belang (en de redelijke verwachting doelbinding).

[27] Art. 25 AVG.

Voor zowel derden als klanten geldt dat:

- betrokkene zich probleemloos (kosteloos en gemakkelijk) moet kunnen afmelden: deze mogelijkheid moet telkens worden geboden, zowel bij het verzamelen van data als bij de verzending van de boodschap;
- Het moet duidelijk zijn wie de afzender is, anonieme mailing is uit den boze.

Verder geeft de ACM nog de volgende aanwijzingen:

- Een persbericht is geen spam, maar als de mailing wordt verzonden naar een grotere groep die niet je doelgroep voor deze mailing is, dan kan het toch weer onder "spam" vallen;
- Voor "*tell a friend*" *viral marketing* gelden specifieke vereisten;
- Iemand die informatie opvraagt is nog geen klant. Deze mag dus ook nog geen nieuwsbrief worden toegezonden behalve als deze daarvoor toestemming heeft verkregen.

Zie voor verdere informatie:

de website van de ACM (autoriteit consument en markt):

https://www.acm.nl/nl/onderwerpen/telecommunicatie/internet

de AP: https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies

https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/direct-marketing

KvK: https://www.kvk.nl/privacy/direct-marketing-en-regelgeving/

Social Media Targeting

Een deel van de inkomsten van social media bestaat uit het aanbieden van gerichte reclame en marketingberichten waarvan men verwacht dat de opbrengst/het effect daarvan het grootste is. socialmediakanalen gebruiken hier data voor die zij zelf bij hun gebruikers verzameld hebben en tevens data die afkomstig zijn van *data brokers*. Hier kunnen nogal wat privacyrisico's aan verbonden zijn, omdat er veel partijen betrokken zijn en voor een buitenstaander lastig vast te stellen is of elke organisatie in deze keten de privacy wel op orde heeft.

Een recent oordeel (2 februari 2022) van de Belgische privacy waakhond heeft het hele systeem van geautomatiseerde online advertentie veiligen op zijn kop gezet. De Belgische Gegevensbeschermingsautoriteit (GBA) heeft aan IAB Europe (het grootste online veilingplatform) een boete van 250.000 opgelegd omdat hun cookiebanner volstrekt onduidelijk was waarvoor de bezoeker toestemming gaf, dus ook niet dat zijn informatie werd doorverkocht aan honderden "realtime" bieders van gepersonaliseerde online advertenties. De GBA beschouwt IAB als "verantwoordelijke" voor de AVG met alle verplichtingen van dien. IAB had echter bijna geen enkele privacy waarborg getroffen.

De trend die als gevolg van deze belangrijke IAB-uitspraak waar te nemen is, is dat partijen hun eigen data en profielen gaan opbouwen uit “first party” cookies: gegevens van hun klanten zelf bij het bezoek van de eigen website / online platform. Daarbij geven de klanten zelf toestemming voor het volgen van gedrag en interesses op de website, en als zij dit niet doen worden alleen “contextuele advertenties” aangeboden.

De Europese Data Protection Board heeft nu concept ***guidelines*** opgesteld waarin duidelijk wordt gemaakt welke eisen de EDPB aan de betrokken partijen stelt. Belangrijk is dat de EDPB de reclamemaker/marketeer én de socialmediapartij gezamenlijk verantwoordelijk houdt, om te waarborgen dat aan de verplichtingen van de AVG is voldaan.

Zij moeten samen een overeenkomst/regeling opstellen waarin de verantwoordelijkheden over en weer worden vastgelegd, met name wat betreft de uitoefening van privacyrechten.

Deze *guidelines* zullen in de loop van 2022 worden vastgesteld, waarna iedere organisatie dus wordt geacht om hiernaar te handelen.

Tip: Wees je ervan bewust dat er regels voor *social targeting* zijn en dat je niet zomaar Facebook of Instragram kunt inschakelen voor een leuke marketingcampagne voor de beoogde doelgroep. Check vooraf met de privacycoördinator (of FG) of dit wel in lijn is met het privacybeleid en de privacy policy, en zorg dat aan de waarborgen van deze *social media targeting guideline*s is voldaan. De Autoriteit Persoonsgegevens geeft nog geen duidelijke samenvatting van deze *guidelines*. De concept-*guidelines* zijn in elk geval gepubliceerd op:

https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf

Een set aan spelregels voor marketing kan bijvoorbeeld zijn:

- Rechtmatigheid en behoorlijkheid: gebruik de data op een zodanige verantwoorde wijze als je zou willen dat een ander ook met jouw data omgaat;
- Altijd transparant zijn over welke data er voor welk (verder) doeleinde worden gebruikt;
- Bij gebruik van technologie altijd kiezen voor *privacy by default* (dus standaard de privacy beschermende instellingen);
- Kritische check van tool/leverancier, de verwerkingsovereenkomst hiermee en controle op toepassing uitgangspunten plaatsvindt;
- Kritische check of uitwisseling met derden / derde landen buiten de EU plaatsvindt;
- Check op toestemming / bestaande klant;
- Periodieke controle op juistheid gegevens, verwijderen gegevens na bewaartermijn.

Een voorbeeld

Grindr case

In 2020 diende de Noorse Consumentenraad een klacht in tegen Grindr. Deze laatste zou persoonsgegevens onrechtmatig met derden delen voor marketingdoeleinden. Het betrof GPS-locatie, IP-adres, advertentie-ID, leeftijd, geslacht en het gegeven dat de gebruiker op Grindr zat. Gebruikers konden worden geïdentificeerd aan de hand van de gedeelde gegevens en de ontvangers konden de gegevens mogelijk verder delen. De "Noorse AP" kwam tot de conclusie:

- *dat Grindr zonder wettelijke basis (grondslag) haar gebruikersgegevens aan derden heeft verstrekt voor gedragsadvertenties;*
- *Verder heeft de autoriteit geconcludeerd dat toestemming in dit geval de toepasselijke rechtsgrondslag was. De beweerdelijke toestemmingen die Grindr verzamelde voor het delen van persoonlijke gegevens met advertentiepartners, waren niet geldig volgens het oordeel van de "Noorse AP". Evenmin was sprake van duidelijke en transparante communicatie met de gebruikers over het delen van persoonsgegevens. De autoriteit is van mening dat dit in strijd was met de AVG-vereisten voor geldige toestemming;*
- *Gegevens waaruit blijkt dat iemand een Grindr-gebruiker is, wijzen er sterk op dat hij tot een seksuele minderheid behoort. Gegevens over iemands seksuele geaardheid vormen bijzondere gegevens die bijzondere bescherming verdienen onder de AVG. Omdat de door Grindr verzamelde toestemmingen niet geldig waren, kon Grindr dergelijke gegevens niet op wettige wijze delen.*

De Noorse Autoriteit Persoonsgegevens heeft een bestuurlijke boete opgelegd van circa € 6,5 miljoen wegens het niet naleven van de AVG-regels inzake toestemming.

13. Cookies

Op het plaatsen van cookies is naast de AVG de Telecommunicatiewet van toepassing. De volgende cookies zijn te onderscheiden:

- **Functionele** cookies zijn altijd toegestaan (om de website te laten functioneren);
- **Analytische** cookies die bezoekersgedrag analyseren: ook hiervoor geldt de Telecommunicatiewet, je moet de bezoeker hierover informeren. Het plaatsen van cookies is pas toegestaan na toestemming van de bezoeker;
- **Tracking cookies** zijn alleen toegestaan indien de medewerker hiervoor ondubbelzinnige toestemming heeft gegeven. Daarvoor moet je de volgende informatie verstrekken: welke informatie je over de bezoeker verzamelt, hoe je die informatie verzamelt: met cookies, scripts of *beacons*, en wat je met die informatie doet;
- Het is niet toegestaan de website achter een "cookiewall" te plaatsen, d.w.z. dat toegang pas mogelijk is na acceptatie van alle cookies;
- Alle cookies waarvoor je toestemming wil verkrijgen moeten worden vermeld in de cookiebanner.

Cookiebanner

Een cookiewall is verboden! De IAB zaak (zie H. 12) heeft ook aangetoond dat een ondoorzichtige en dwingende cookiebanner waardoor bezoekers op "accepteer alle cookies" klikken om naar de website te kunnen, anno 2022 echt niet meer kan. Onderwerp je cookiebanner dus tijdig aan een kritisch onderzoek. Geef de bezoeker een makkelijke keuze voor "accepteren", "afwijzen" en vermeld bij "bekijk doeleinden" voor welke doeleinden je de data verzamelt.

Analytische cookies

De meest bekende analytische cookies zijn Google Analytics. Deze worden door veel bedrijven gebruikt voor hun websites. Echter, op 22 december 2021 heeft de Oostenrijkse privacytoezichthouder geconcludeerd dat Google Analytics strijdig met de AVG is nu Google IP-adressen en cookiegegevens naar de VS stuurt. De Franse CNIL volgde op 10 februari 2022.

Dit naar aanleiding van een klacht van advocaat en privacy-activist Schrems. Schrems is al sinds 2011 bezig met klachten tegen Facebook en hun uitwisseling van persoonlijke data van Facebookgebruikers naar de Verenigde Staten. Hierdoor konden ook Amerikaanse veiligheidsdiensten (NSA) onbekommerd rondsnuffelen in gegevens van Facebookgebruikers, iets wat onthuld werd door Edward Snowden. In het Schrems I arrest werden de "Safe Harbour" Agreement met de VS ongeldig verklaard: de VS konden de privacy niet waarborgen. Hierna is een nieuw systeem "Privacy Shield" afgesproken tussen de EU en de VS. Echter ook hiertegen diende Schrems klachten in en ook nu werd hij in het gelijk gesteld.

Nadat het Privacy Shield ongeldig was verklaard - Schrems II (16 juli 2020) - heeft Schrems vele klachten ingediend bij diverse nationale toezichthouders over de uitwisseling van data naar de VS ondanks ontbrekende privacywaarborgen. Zie voor meer informatie over Schrems en zijn organisatie NYOB (my privacy is none of your business): https://noyb.eu/en

De AP heeft haar standpunt inzake Google Analytics weliswaar aangescherpt maar heeft Google Analytics vooralsnog niet verboden. De AP waarschuwt echter nadrukkelijk dat dit verbod nog steeds kan volgen. Voor nu geeft de AP tips om Google Analytics zoveel mogelijk privacyvriendelijk in te stellen:

- sluit een actuele (nieuwe) verwerkersovereenkomst met Google (via accountinstellingen);
- verwerk de laatste 8 cijfers van het IP-adres niet; (“anyomize IP”),
- Zet het delen van gegevens met Google uit;
- Zet het delen van gegevens met Google voor advertentiedoeleinden uit;
- Schakel de functie user ID uit (volgen naar andere *devices*, meerdere sessies);
- Laat de bezoeker weten dat je Google Analytics gebruikt.

Zie voor de gehele handleiding:

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleiding_privacyvriendelijk_instellen_google_analytics.pdf

Tracking cookies

Deze cookies volgen het online gedrag van mensen en slaan de interesses van hen op, ook nadat zij de betreffende website hebben verlaten. Deze cookies mogen alleen worden geplaatst als de bezoeker hiervoor toestemming heeft gegeven. Doel hiervan is o.a. om zoveel mogelijk informatie te verzamelen op basis waarvan gerichte advertentie/marketing kan worden voorgeschoteld. Op de achtergrond worden al deze gegevens “big data” verwerkt en profielen bijgehouden van iedereen die het internet bezoekt.

Gezien deze vergaande monitoring en profiling is toestemming dus vereist. Maar wie weet nu echt waarvoor hij/zij toestemming heeft gegeven? Meestal klik je de cookiebanner snel weg, alleen al omdat het te ingewikkeld of tijdrovend is om slechts toestemming voor noodzakelijke cookies te geven. Zeker van kinderen kan niet verwacht worden dat zij begrijpen waar zij mee instemmen.

De EDPD (de gezamenlijke privacytoezichthouders van de EU) heeft in november 2021 een oproep gedaan om strengere regels te stellen aan tracking cookies en deze uiteindelijk te gaan verbieden. Dit is dus iets om mee rekening te houden bij het maken van beleidskeuzes in de online marketing.

Gelet op deze ontwikkelingen zouden realistische (kritische) eisen die anno 2022 aan de cookies kunnen worden gesteld, zijn dat deze:

- Uitsluitend tot doel hebben het meten van het publiek van de eigen site of applicatie (prestatiemeting, detectie van browseproblemen, optimalisatie van technische prestaties of de ergonomie ervan, schatting van het vermogen van de vereiste servers, analyse van geraadpleegde inhoud), voor de exclusieve rekening van de uitgever;
- alleen worden gebruikt om anonieme statistische gegevens te produceren (dus noodzakelijk en beperkt statistisch);
- niet leiden tot een kruiscontrole van de gegevens met andere verwerkingen;
- niet leiden tot het doorgeven van de gegevens aan derden (“third party” cookies);
- niet het algemene browsen volgen van een bezoeker die verschillende applicaties gebruikt of op verschillende websites surft;
- Geen gebruik van een *identifier* op meerdere sites (via bijvoorbeeld cookies die zijn geplaatst op een website van derden dat door verschillende sites wordt geladen) om een uniforme dekkingsgraad ("bereik") van een inhoud te kruisen, dupliceren of meten.

14. Privacyrechten betrokkenen

In de AVG zijn de rechten van "betrokkenen" op wie de persoonsgegevens betrekking hebben, sterk verbeterd en uitgebreid. Doel van deze rechten is dat er een effectieve bescherming van persoonsgegevens wordt bereikt. Mensen hebben het recht om te weten door wie, en op welke wijze hun gegevens worden verwerkt. Het is verstandig om de processen en interne organisatie in te richten op deze rechten:

- **Recht van bezwaar:**[28] o.a. tegen een verwerking vanwege specifieke persoonlijke omstandigheden; tegen direct marketing, online *behavorial* advertising; bij wetenschappelijk, historisch onderzoek of statistische doeleinden (op grond van specifieke persoonlijke omstandigheden). De verwerkingsverantwoordelijke zal via belangenafweging moeten motiveren of en waarom de verwerking alsnog rechtmatig is.

- **Informatieplicht**[29] jegens de betrokkene, welke gegevens van hem/haar worden verzameld (zowel door diegene die de gegevens van de betrokkene heeft verkregen als degene die de gegevens niet van de betrokkene heeft verkregen).

- **Recht op inzage**[30]: op verzoek verstrekken van informatie welke gegevens worden verwerkt zodat de betrokkene kan controleren of deze juist zijn en op rechtmatige wijze worden verwerkt. De aangewezen vorm is "elektronische inzage", dus zoveel als mogelijk digitale toegang tot een beveiligd systeem waarin de betrokkene meteen zijn gegevens kan inzien. Let op, daarbij moet de organisatie ook de rechten en vrijheden van anderen beschermen, dus alle persoonsgegevens die niet de betrokkene betreffen moeten worden afgeschermd/geanonimiseerd. Er mogen geen kosten voor in rekening worden gebracht. Wel kan een herhaald of onredelijk (te arbeidsintensief, te kostbaar) verzoek worden afgewezen. Daarnaast bestaan nog twee andere weigeringsgronden: openbare veiligheid en om strafbare feiten te voorkomen of op te sporen.

Ter info: de EDPB heeft eind januari 2022 nieuwe *guidelines* vastgesteld over wat de scope van het inzagerecht precies inhoudt, wat de verantwoordelijke moet doen bij een inzageverzoek en een format voor inzageverzoeken. Deze worden binnenkort gepubliceerd op de website van de EDPB.

- **Recht op rectificatie**[31]: het recht op onverwijlde correctie van onjuiste gegevens (met inachtneming van de doeleinden van de verwerking).

- **Recht op gegevenswissing** ("vergetelheid")[32] het recht op zonder onredelijke vertraging te wissen indien:
- de gegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld;
- de betrokkene de toestemming intrekt en er geen andere rechtsgrond (grondslag) is voor de verwerking;

[28] Art. 21 AVG.
[29] Art. 12, 13 en 14 AVG.
[30] Art. 15 AVG.
[31] Art. 16 AVG.
[32] Art. 17 AVG.

- de betrokkene bezwaar maakt tegen de verwerking. De verantwoordelijke moet de verwerking staken tenzij er dwingende gerechtvaardigde gronden zijn die zwaarder wegen dan de belangen van betrokkene;
- de gegevens onrechtmatig verwerkt zijn;
- de gegevens op basis van een wettelijke verplichting gewist moeten worden;
- het gegevens betreft van een kind, verzameld in het kader van diensten van de informatiemaatschappij.
  Let op: het recht op onvergetelheid is niet onbegrensd, sommige gegevens kunnen niet worden gewist omdat er een wettelijke (fiscale) verplichting is om de gegevens gedurende de bewaartermijn te bewaren.[33]

- **Recht op dataportabiliteit[34]:** Het recht om persoonsgegevens over te laten dragen aan een andere partij.

- **Het recht op beperking van de verwerking[35]:** Ingeval van een dispuut: het recht om minder gegevens te laten verwerken c.q. het opschorten van de verwerking.

- **Het recht met betrekking tot geautomatiseerde besluitvorming en profilering[36]:** Oftewel: het recht op menselijke beoordeling bij besluiten. Organisaties kunnen op basis van geautomatiseerde besluitvorming een beslissing nemen met persoonlijke gevolgen. Bijvoorbeeld: het afwijzen van een kredietaanvraag. Op basis van de AVG heb je het recht op een nieuw besluit waarbij wel sprake is van beoordeling door een mens. Geautomatiseerde besluitvorming moet voldoen aan strenge voorwaarden.

  Let op: Bij de uitoefening van privacyrechten moet de verwerkingsverantwoordelijke de **identiteit** van betrokkene controleren, voordat hierop in kan worden gegaan.[37]

- **Transparantiebeginsel[38]**: de verwerkingsverantwoordelijke (de organisatie) zorgt ervoor dat in heldere taal en toegankelijke vorm wordt gecommuniceerd over de privacyrechten van betrokkene. Voordat de organisatie voldoet aan een verzoek om inzage, verwijderding, enz. zal in bepaalde gevallen eerst de identiteit van de verzoeker worden vastgesteld.

Actiepunten

- Het is belangrijk om in de privacy policy (op de website) een hoofdstuk te wijden aan privacyrechten, en hoe deze uit te oefenen;
- Nu de organisatie dergelijke verzoeken moet vergemakkelijken/faciliteren is het raadzaam hier een werkwijze / protocol voor te hebben. Denk aan zaken als: wie ontvangt het, wie handelt het af, welke gegevens kunnen worden verstrekt, binnen welke termijn, en bijvoorbeeld een standaardformulier om af te lopen;
- De uitoefening van privacyrechten onderstreept de noodzaak om alle gegevens op een gestructureerde, systematische manier op te slaan (zodat het gemakkelijk is terug te

[33] Art. 17 lid 3 AVG.
[34] Art. 20 AVG.
[35] Art. 18 AVG.
[36] Art. 21 en 22 AVG.
[37] Art. 12 lid 6 AVG.
[38] Art. 12, 13, 14 AVG.

vinden, over te dragen,na afloop bewaartermijn te wissen), en zelf altijd te werken volgens de beginselen van datakwaliteit en dataminimalisatie.

Zie voor meer informatie:

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/rechten-van-betrokkenen?qa=rechten

15. Bewaartermijnen

Voor alle verwerkingen moet de organisatie zich afvragen of de gegevens daadwerkelijk bewaard moeten worden en zo ja voor hoelang. Dit op basis van het beginsel van "**opslagbeperking**"[39]. Is er nut en noodzaak om de gegevens te bewaren, dan moet je bepalen welke bewaartermijnen gelden. Zowel de motivatie c.q. belangenafweging voor de bewaartermijn als de termijn zelf, leg je vast in intern beleid voor bewaartermijnen. Zodra de termijn verloopt, mag je de gegevens niet meer verwerken tenzij voor een ander, daarmee verenigbaar doel.

Er zijn ook wettelijke bewaartermijnen waar je je in elk geval aan moet houden. Dit geldt voor bijvoorbeeld personeelsdossiers (twee jaar) salarisadministratie (zeven jaar), de financiële administratie (veelal zeven jaar) en onroerend goed (tien jaar). Hiertoe moet je per onderwerp de wettelijke/fiscale bewaartermijn vaststellen. Kijk bijvoorbeeld op de website van de Belastingdienst:

https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/zakelijk/ondernemen/administratie/een_administratie_opzetten

Een overzicht van bewaartermijnen vind je ook hier: https://www.awvn.nl/hr-van-a-tot-z/privacy-bewaartermijn-personeelsgegevens/

- Duidelijkheid: om te komen tot een eenduidige werkwijze bij het bewaren van data, is het verstandig om alle bewaartermijnen in het privacybeleid op te nemen, en in het verwerkingenregister per verwerking.
- *Privacy by design*: Het is handig om de bewaartermijn al automatisch te laten verwerken in de bedrijfsprocessen / software door *privacy by design*: het automatisch vernietigen van data na afloop van de bewaartermijn, tenzij je deze apart hebt opgeslagen:
- Markeren bijzondere informatie/afwijkende bewaartermijn (labelen): Als een afwijkende bewaartermijn geldt, moet de informatie ook apart worden opgeslagen of gelabeld. Dit is bijvoorbeeld nodig bij het werken met gevaarlijke stoffen, data over een (bedrijfs)ongeval, een potentiële aansprakelijkheid waarvoor je zowel voor de betrokkenen als voor de (rechts) positie van de organisatie de relevante informatie langer moet bewaren. In dit geval geldt de termijn waarna de wettelijke aansprakelijkheid afloopt.

Verwijderen betekent natuurlijk dus ook écht vernietigen en niet "een beetje". Zorg voor een veilige methode. Laptops en mobiele telefoons moeten echt geschoond zijn van data, schakel hiervoor ICT, een externe tool of een gespecialiseerde partij in.

[39] Art. 5 lid 1 sub e AVG.

16. Datalek

Het overkomt veel organisaties: een datalek. Dit kan van alles zijn, zoals een mail naar het verkeerde mailadres, een dossier in de trein laten liggen, het verliezen van een usb-stick, personeel dat op de verkeerde link klikt in een mail (*phishing, malware, ransomware*) of een *hack*.

"Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie, zonder dat dit de bedoeling is van deze organisatie." (aldus de AP).

Heb je onverhoopt met een datalek te maken, dan is het **belangrijk om snel in actie te komen! Iedereen moet op de hoogte zijn van wat er moet gebeuren. Stel hiervoor een werkwijze op (datalekprotocol).** Zie voor een stappenplan van de AP: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stappenplan_actie_datalek.pdf

Melden AP Het is belangrijk om te weten dat een datalek bijna altijd bij de AP moet worden gemeld om een boete wegens niet melden te voorkomen. Dit is alleen anders als het datalek geen risico voor de rechten en vrijheden van betrokkenen oplevert.[40]

De melding moet binnen 72 uur, althans zonder onredelijke vertraging, bij de AP worden gedaan. Als de melding later plaatsvindt, moet dit goed gemotiveerd worden. De AP kan onderzoeken of de beveiliging op orde was. Als dit niet het geval is, kan de AP een boete opleggen wegens onvoldoende beveiligingsmaatregelen.

Let op: de AP vraagt bij het doen van de melding ook meteen om de onderzoeksrapportage en een kopie van de melding aan betrokkenen (indien aan de orde).

Melden aan betrokkenen is verplicht als dit datalek een hoog risico inhoudt[41]: als dit kan leiden tot lichamelijke, materiële of immateriële schade voor de betrokken personen. Bijvoorbeeld als het om bijzondere of gevoelige informatie gaat (bijvoorbeeld BSN- of bankrekeningnummer, ras, geloof, seksuele geaardheid, medische of strafrechtelijke gegevens), of als het om een combinatie van persoonlijke gegevens gaat, waarmee identiteitsfraude kan worden gepleegd.

De melding aan betrokkenen moet onverwijld gebeuren (zodat de betrokkene de schade zoveel mogelijk kan beperken) en bevat in duidelijke taal de volgende informatie:

1. Wat is er met de gegevens gebeurd?
2. Zijn er gegevens in handen van onbevoegden gevallen, tijdelijk of permanent ontoegankelijk geworden?
3. Om welke gegevens gaat het?
4. Is er risico op lichamelijke of immateriële schade als gevolg van het datalek?
5. Zijn de gegevens in handen van een kwaadwillende?
6. Zijn de gegevens inmiddels vernietigd of weer teruggestuurd?
7. Vermeld de maatregelen die je hebt getroffen teneinde het lek te dichten en hoe dit in de toekomst zal worden voorkomen. Vermeld of je hierbij externe hulp of advies hebt gehad;
8. Adviseer individuele maatregelen die de betrokkene kan treffen om het risico op schade te verkleinen (bijvoorbeeld bij identiteitsfraude);
9. Geef de naam op van de FG (functionaris voor gegevensbescherming) / privacycoördinator / directeur van de organisatie, zodat betrokkenen nadere vragen kunnen stellen.

[40] Art. 33 AVG.
[41] Art. 34 AVG.

Deze melding aan de betrokkenen komt grotendeels overeen met de melding aan de AP, met het verschil dat hier niet verplicht is om te melden welke categoriën betrokkenen en hoeveel betrokkenen het betreft.

Elk datalek (hoe klein ook) moet intern worden geregistreerd in het datalekregister: hierbij wordt dezelfde informatie opgenomen als hierboven vermeld. Zie ook:

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/10_tips_datalekregistratie.pdf

https://www.cip-overheid.nl/media/1143/20170126_meldplicht_v2_2-def.pdf

17. Verwerker / verwerkersovereenkomst

Onderscheid **verwerkingsverantwoordelijke / verwerker**: de organisatie is **verwerkingsverantwoordelijke** wanneer men simpel gezegd voor de bedrijfsactviteiten persoonsgegevens verwerkt of doet verwerken. Hij bepaalt daarbij zelf welke soort gegevens hij verwerkt, hoe lang en met welke middelen.[42]

Als de organisatie van haar eigen bedrijfsactiviteiten bepaalde taken door anderen laat uitvoeren zoals beveiliging, ICT, ticketing, transport, mailing of software, dan is deze derde doorgaans de "verwerker": hij verwerkt persoonsgegevens namens de verantwoordelijke. Met de verwerker moet een "verwerkersovereenkomst" worden gesloten opdat de privacy ook gewaarborgd is bij deze derde. Zie hiervoor ook:

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/voorbeeldlijst_verwerkers_def.pdf

Er kunnen ook meerdere verwerkingsverantwoordelijken **gezamenlijk verantwoordelijk** zijn.[43] Bijvoorbeeld als meerdere organisaties een samenwerkingsverband aangaan voor het verzamelen, opslaan en verwerken van persoonsgegevens. Deze organisaties zijn dan samen in staat de doeleinden en middelen van de verwerkingen vast te stellen.

Nu de verwerkingsverantwoordelijke altijd "verantwoordelijk" blijft voor de privacywaarborgen, vloeit hier ook een verplichting uit voort om met alle "verwerkers" een **verwerkersovereenkomst** te sluiten. Hoe deze er precies uitziet, mag verschillen per organisatie en branche omdat de AVG open normen bevat. Echter de Autoriteit Persoonsgegevens adviseert om in elk geval te checken of de punten uit artikel 28 lid 3 AVG geregeld zijn.

De brancheorganisatie NLDigital heeft voor haar leden een gedragscode opgesteld die is goedgekeurd door de AP. Deze is geschreven voor alle IT-leveranciers die als verwerker met data omgaan van de opdrachtgever. Check of de IT-leverancier zich hieraan heeft gecommitteerd. De gedragscode geeft ook algemeen een goed beeld wat je met de verwerker kunt regelen in de verwerkersovereenkomst: https://www.nldigital.nl/data-pro-code/

Checklist Verwerkersovereenkomst (art. 28 lid 3 AVG):

De verwerker:

a) verwerkt de persoonsgegevens uitsluitend op basis van schriftelijke instructies van de verwerkingsverantwoordelijke, onder meer met betrekking tot doorgiften van persoonsgegevens aan een derde land of een internationale organisatie;
b) stelt de verwerkingsverantwoordelijke onmiddellijk in kennis indien naar zijn mening een instructie inbreuk oplevert op de AVG of op andere Unierechtelijke of wettelijke bepalingen inzake gegevensbescherming;
c) waarborgt dat de geautoriseerde medewerkers zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden;
d) neemt alle vereiste beveiligingsmaatregelen (artikel 32 AVG);

[42] Art. 24 AVG.
[43] Art. 26 AVG.

e) schakelt geen subverwerker in dan na goedkeuring van de verantwoordelijke en sluit met de subverwerker een (sub)verwerkersovereenkomst;
f) voor zover mogelijk, faciliteert privacyrechten betrokkenen, rekening houdend met de aard van de verwerking, de verwerkingsverantwoordelijke door middel van passende technische en organisatorische maatregelen;
g) verleent bijstand aan verwerkingsverantwoordelijke voor zover redelijkerwijs mogelijk/verlangd kan worden bij beveiliging, melding van inbreuk aan toezichthouder en betrokkene, een gegevenseffectbeschermingsbeoordeling (art. 32-35 AVG);
h) is verplicht om na afloop van het contract, de persoonsgegevens naar keuze van de verantwoordelijke terug te bezorgen dan wel te wissen en kopieën te verwijderen, tenzij opslag van de persoonsgegevens wettelijk is verplicht;
i) stelt aan de verwerkingsverantwoordelijke alle informatie ter beschikking die nodig is om de nakoming van de in dit artikel neergelegde verplichtingen aan te tonen en maakt mogelijk dat de verantwoordelijke of gemachtigde controleur *audits*, waaronder inspectiesen aan bijdraagt.

Wat hoort (bijvoorbeeld) niet thuis in een verwerkersovereenkomst:

- Aansprakelijkheid uitsluiten of beperken voor schade als gevolg van handelwijze in strijd met AVG;
- Aansprakelijkheid voor boetes AP uitsluiten / verleggen;
- Contractuele afspraken over de dienst of het product zelf, deze horen in het contract en niet in de verwerkersovereenkomst.

18. Verstrekken gegevens aan derden/buiten EU

Als jouw organisatie gegevens wil uitwisselen met derden (leveranciers), dan moet je nagaan of dit binnen de grondslag gerechtvaardigd is en binnen doelbinding (en redelijkerwijs verder te verwachten verwerking) valt op basis waarvan je de gegevens hebt verkregen.[44]

Rechtmatige grondslag:

- is de grondslag alleen toestemming, dan dient de betrokkene dus ook toestemming te hebben gegeven voor de verstrekking van gegevens aan de derde / buiten de EU en met kennis van de mogelijke risico's;
- uitvoering van een overeenkomst, mits het om een incidentele uitwisseling gaat die strikt noodzakelijk is;
- Bij gerechtvaardigd belang moet er een belangenafweging plaatsvinden waarbij het (commerciële) belang van de verantwoordelijke wordt afgewogen tegen dat van de betrokkene, moet worden onderzocht of op een minder invasieve wijze hetzelfde doel kan worden bereikt en of de fundamentele rechten en vrijheden van betrokkene niet moeten prevaleren.

Doelbinding: valt de verwerking niet meer binnen het oorspronkelijke doel, dan moet worden bepaald of het andere doel nog te verenigen is met het oorspronkelijke doel. De AP noemt de volgende factoren die daarbij een rol kunnen spelen:

- *ieder verband met het doel van verzamelen;*
- *het kader waarin de persoonsgegevens zijn verzameld (verhouding betrokkenen en verwerkingsverantwoordelijke);*
- *de aard van de gegevens (bijzondere persoonsgegevens en/of persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten);*
- *de (mogelijke) gevolgen van een verstrekking;*
- *het bestaan van passende waarborgen (o.a. versleuteling of pseudonimisering);*
- *de verwachtingen van de betrokkene (degene van wie een organisatie persoonsgegevens gebruikt).*
  (https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/verstrekken-van-persoonsgegevens)

Verwerkers/gegevensuitwisselingovereenkomst: vervolgens moet er een adequate verwerkers- of gegevensuitwisselingsovereenkomst worden gesloten.[45] Een gegevensuitwisselingsovereenkomst sluit je als beide partijen "verantwoordelijke" zijn ten aanzien van de persoonsgegevens. In elk geval leg je met deze overeenkomst vast hoe deze leverancier / samenwerkende partij met de persoonsgegevens omgaat en welke waarborgen er worden gegeven om er zeker van te zijn dat de AVG goed wordt nageleefd. Zie H. 17 inzake "Verwerker".

Informatieplicht: De betrokkene moet duidelijk worden geïnformeerd over de uitwisseling van data met derden ("ontvangers") / buiten de EU (en in dit laatste geval, ook of sprake is van een adequaatheidsbesluit, *binding corporate rules* of passende waarborgen, zie hieronder). Dit zodat zij hierover ook hun "controle" en privacyrechten kunnen uitoefenen.

[44] Art. 44 AVG.
[45] Art. 28 AVG.

Uitwisseling buiten EU/EER

Uitwisseling binnen de EU en EER (inclusief Noorwegen, Liechtenstein, IJsland) wordt - dankzij de AVG - als een uitwisseling naar een land met een passend beschermingsniveau beschouwd. Ook buitenlandse bedrijven die in Europa gevestigd zijn dienen zich volledig aan de AVG te houden. Maar daarnaast vindt er ook veel data-uitwisseling plaats met landen buiten de EU. Als dat binnen een bedrijf gebeurt, dan kan het bedrijf hiervoor ***"Binding Corporate Rules"*** opstellen waaraan het zich moet houden. Deze moeten worden goedgekeurd door de nationale autoriteit en/of de EDPB.[46] Zie hiervoor verder: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en#approval-of-binding-corporate-rules

Stel dat het niet binnen het concern gebeurt, maar dat persoonsgegevens worden gedeeld met een "derde" land. Dan moet je onderzoeken of dit derde land een "**passend beschermingsniveau**" biedt, vergelijkbaar met de AVG. Over bepaalde landen heeft de Europese Commissie een "adequaatheidsbesluit" genomen waarmee je ervan verzekerd bent dat dit land een passend beschermingsniveau biedt, vergelijkbaar met de AVG.[47] Dat zijn op dit moment slechts 13 landen (Andorra, Argentinië, Canada (alleen commerciële organisaties), Faeröer Eilanden, Guernsey, Isle of Man, Israël, Japan, Jersey, Nieuw-Zeeland, Uruguay, Verenigd Koninkrijk, Zwitserland, zie ook: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal/doorgifte-binnen-en-buiten-de-eu#wanneer-mag-ik-persoonsgegevens-doorgeven-naar-de-vs-5539).

Uitwisseling met derde landen: passende waarborgen

Modelcontract/SCC: Voor de rest van de wereld geldt dus dat contractueel passende waarborgen moeten worden afgedwongen.[48] De EDPB heeft hiervoor modelcontracten opgesteld, en per november 2021 geüpdatet (SCC, *Standard Contractual Clauses*). Deze moet je ongewijzigd overnemen om ze geldig te laten zijn. Als je aanpassingen of aanvullingen wilt, moet je hiervoor toestemming vragen bij de AP.

Data Transfer Impact Assessment: Als aanvullende eis moet je per land en situatie beoordelen of de uitwisseling van gegevens wel verantwoord plaats kan vinden:

https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

Uitwisseling met VS / Schrems II

VS als **derde land**: op 16 juli 2020 heeft het Europese Hof het Privacy Shield van de VS ongeldig verklaard, met name omdat Amerikaanse inlichtingen- en veiligheidsdiensten onbeperkte toegang hadden tot de persoonsgegevens van Europese burgers. Ook heeft zij geoordeeld dat de Amerikaanse wetgeving geen passend beschermingsniveau biedt. Dit dankzij Schrems, die eerder al de uitwisseling van gegevens van Facebook Ierland met Facebook VS aan de kaak had gesteld. Ook toen bleken de Amerikaanse inlichtingendiensten vrij te beschikken over de gegevens van Europese burgers. Dit kwam

[46] Art. 47 AVG.
[47] Art. 46 AVG.
[48] Art. 46 AVG.

aan het licht door Edward Snowden. In deze zaak sneuvelde de "*Safe Harbour Principles*" die met de VS waren afgesproken.

Op dit moment geldt er dus geen algemene waarborg om gegevens met de VS uit te wisselen. De VS en de Europese Commissie hebben inmiddels wel een voornemen voor nieuwe afspraken, maar is er nog geen nieuw akkoord. De VS is kortom vooralsnog een "derde land". Uitwisseling van persoonsgegevens met de VS kan op dit moment alleen via een van de **modelcontracten** van de EDPB. Vervolgens moet er dus ook nog een **Data Transfer Impact Assessment** worden uitgevoerd (DTIA).

Als je met een partij als Google werkt, maar ook bij oplossingen in de *cloud*, check dan de verwerkersovereenkomst en zoek uit of de verwerker de gegevens buiten de EU wil uitwisselen. Als hiervoor geen grondslag, modelcontract en DTIA is gehouden (en deze ruimte is dus zeer beperkt!!!) **dan moet in een clausule worden vastgelegd dat de verwerker de gegevens niet uitwisselt buiten de EU**.

Actiepunt: breng alle data-uitwisselingen met derde landen in kaart en controleer of alle bovenstaande stappen zijn doorlopen.

Zie voor meer informatie: https://edpb.europa.eu/sites/default/files/files/file1/edpb_faqs_schrems_ii_202007_adopted_nl.pdf

19. Nuttige websites

European Data Protection Board: https://edpb.europa.eu/edpb_nl

Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/

Autoriteit Consument en Markt: https://www.acm.nl/nl

Rijksoverheid: https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens

Kamer van Koophandel (KvK): https://www.kvk.nl/advies-en-informatie/wetten-en-regels/privacywetgeving-avg-wanneer-ben-je-compliant/

Centrum Informatiebeveiliging en Privacybescherming: https://www.cip-overheid.nl/

Public Spaces: ethiek en tools voor privacy: https://publicspaces.net/

Belgische Gegevensbeschermingsautoriteit: https://gegevensbeschermingsautoriteit.be/burger

Franse privacy autoriteit: https://www.cnil.fr/en/home

Website my privacy is none of your business (van Max Schrems): https://noyb.eu/en

Dit naslagwerk is geschreven in opdracht van de Taskforce Samenwerkingsverband Publieksdata. Het bevat geen juridisch advies. Het is geschreven eind 2021/begin 2022 en betreft dan ook een momentopname van de stand van zaken begin 2022. Feedback voor verbetering is altijd welkom en kan worden gestuurd aan publieksdata@den.nl.

Cineville, CJP, Digitaal Informatieplatform Podiumkunsten (DIP), Kunsten ’92, Platform ACCT en Rotterdam Festivals vormen de Taskforce Samenwerkingsverband Publieksdata onder leiding van DEN Kennisinstituut cultuur & digitale transformatie. De taskforce wordt mede mogelijk gemaakt door het Ministerie van OCW. Kijk voor meer informatie op www.publieksdata.nl