TOEPASBAARHEID AVG WETGEVING VERTELKNUFFEL SAMBUDDY

Auteur: Tamim Mohtasebzada

Inhoudsopgave

1. Inleiding

In dit document wordt de AVG privacy wetgeving toegelicht. Er komen een aantal grondslagen aan bod waarop bedrijven of organisaties kunnen verklaren waarom ze beeld- of audio opnamen maken. Verder wordt er in een klein stukje toegelicht hoe de stakeholder(s) het eerste prototype hebben aangepakt.

2. Wat is de AVG wetgeving?

De privacywet Algemene Verordening Gegevensbescherming (AVG) geldt sinds 25 mei 2018 voor de hele Europese Unie. Internationaal heet de wet General Data Protection Regulation (GDPR). Door de wet AVG heb je meer verplichtingen bij het verwerken van persoonsgegevens dan voorheen. De privacyrechten zijn met de AVG versterkt en uitgebreid. Gebruikers (zoals je klanten) hebben met de AVG meer mogelijkheden om voor zichzelf op te komen als het gaat om de verwerking van hun gegevens. Zij hebben meer zeggenschap over hun gegevens en wat bedrijven daar mee doen. Je klant kan bijvoorbeeld inzage vragen in opgeslagen data, of verleende toestemming intrekken (den Breejen, 2021).

2.1 Voor wie geldt de AVG?

De Europese privacywet geldt voor alle bedrijven en organisaties die persoonsgegevens vastleggen van klanten, personeel of andere personen uit de EU. Vrijwel alle ondernemers hebben ermee te maken, ook zzp'ers en mkb. De wet geldt ook voor scholen, zorginstanties, verenigingen en stichtingen. Internationale bedrijven die zakendoen met de EU moeten zich houden aan de AVG.

De omvang van je bedrijf en de aard van de activiteiten bepalen welke AVG-maatregelen je neemt. Je krijgt er al mee te maken door het uitsturen van een offerte, factuur, en (digitale) nieuwsbrief. Of door het bijhouden van afspraken met klanten, contactgegevens van klanten of personeelsinformatie. Daarnaast vallen ook gegevens gekoppeld aan IP-adressen, cookies, een e-mailadres onder de wet. Ook als je niet weet wie er schuilgaat achter deze gegevens moet je ze als privacygevoelig behandelen.

In Nederland houdt de Autoriteit Persoonsgegevens (AP) toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens. In 2019 dienden ruim 27.800 mensen er een klacht in vanwege een mogelijke privacyschending. Aleid Wolfsen, voorzitter van de AP: "AVG is weliswaar ingewikkelde materie, maar gebruik ook je gezond verstand. Heb ik deze data echt nodig? En mag ik deze data zomaar gebruiken of moet ik om toestemming vragen? Dan kom je al een heel eind met de vraag wat wel en niet mag."

2.2 Regelhulp AVG

De Regelhulp AVG van de AP helpt je bij het bepalen van de impact van de AVG op jouw bedrijf. Hierin staan onderstaande 10 vragen. Na het beantwoorden van deze vragen kun je direct aan de slag.

1. **Welke persoonsgegevens verwerk je?**
   Inventariseer welke persoonsgegevens je verwerkt. Persoonsgegevens zijn alle gegevens die direct over iemand gaan of die naar iemand te herleiden zijn, zoals naam, adres, telefoonnummer en burgerservicenummer.

Naast 'gewone' persoonsgegevens zijn er ook bijzondere persoonsgegevens. Deze gaan onder meer over iemands gezondheid, strafrechtelijke verleden of politieke voorkeur. Het is verboden om bijzondere persoonsgegevens te gebruiken, tenzij je een wettelijke uitzondering hebt.

2. **Heb je een grondslag om persoonsgegevens te verwerken?**
   Je mag alleen persoonsgegevens verwerken wanneer je deze echt nodig hebt om je doel te bereiken en het niet anders kan. Je moet dus een goede reden, ofwel 'grondslag' hebben. Bijvoorbeeld dat je toestemming hebt van de persoon om wie het gaat. Of omdat het noodzakelijk is om een overeenkomst uit te voeren. Er zijn 6 grondslagen in de AVG. Het gaat om de volgende 6 grondslagen:

   1. U heeft toestemming van de persoon om wie het gaat
   2. Het is noodzakelijk om gegevens te verwerken om een overeenkomst uit te voeren.
   3. Het is noodzakelijk om gegevens te verwerken omdat u dit wettelijk verplicht bent.
   4. Het is noodzakelijk om gegevens te verwerken om vitale belangen te beschermen.
   5. Het is noodzakelijk om gegevens te verwerken om een taak van algemeen belang of openbaar gezag uit te oefenen.
   6. Het is noodzakelijk om gegevens te verwerken om uw gerechtvaardigde belang te behartigen.

3. **Heb je een functionaris gegevensbescherming nodig?**
   Sommige organisaties moeten een functionaris voor de gegevensbescherming aanstellen. Dit is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG. Deze functionaris is verplicht bij:

   - Overheden en publieke organisaties.
   - Organisaties en bedrijven die vanuit hun kernactiviteiten op grote schaal individuen volgen. Denk hierbij aan cameratoezicht en monitoring van iemands gezondheid via wearables.
   - Organisaties en bedrijven die op grote schaal bijzondere persoonsgegevens verwerken en voor wie dit een kernactiviteit is. Bijzondere persoonsgegevens zijn bijvoorbeeld gegevens over iemands gezondheid, ras, politieke opvatting, geloofsovertuiging of strafrechtelijke verleden.

4. **Ben je verplicht om een data protection impact assessment uit te voeren?**
   Bij het verwerken van gegevens met een hoog privacyrisico is een data protection impact assessment (DPIA) verplicht. Blijkt uit de analyse dat de privacyrisico's hoog zijn, dan kun je maatregelen nemen om deze te verkleinen. Een DPIA moet je in ieder geval uitvoeren als je:

   - Bijzondere persoonsgegevens als ras, godsdienst, gezondheid, politieke opvattingen, genetische – of biometrische gegevens op grote schaal verwerkt.
   - Op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied, bijvoorbeeld met cameratoezicht.
   - Gegevens zo combineert, dat iemand in een bepaalde categorie of groep is in te delen en daardoor zo kan worden benaderd of beoordeeld (profilering).

5. **Werk je volgens de uitgangspunten van privacy by design en privacy by default?**
   Zorg ervoor dat je in de ontwerpfase van nieuwe producten of diensten persoonsgegevens goed beschermt. Dit wordt ook wel 'privacy by design' genoemd. Daarnaast moeten de standaardinstellingen de privacy van iemand respecteren (privacy by default) totdat de persoon zelf toestemming geeft. Je mag bijvoorbeeld geen (web)formulier gebruiken waarop al een vakje is aangevinkt.

6. **Moet je een register van verwerkingsactiviteiten opstellen?**
   In een verwerkingsregister neem je op welke persoonsgegevens je gebruikt, voor welk doel, waar je ze opslaat en met wie je ze eventueel deelt. Je bent verplicht om met een register te werken als jouw organisatie:

   - Persoonsgegevens verwerkt waarvan de verwerking meer dan incidenteel is.
   - Risicovolle persoonsgegevens verwerkt, zoals gegevens over gezondheid, godsdienst of politieke opvattingen.
   - Meer dan 250 medewerkers heeft.

   In de praktijk zullen (vrijwel) alle organisaties verplicht zijn zo'n verwerkingsregister AVG bij te houden. Dit komt omdat binnen een organisatie vaak klanten-, leveranciers- of personeelsbeheer voorkomt. Als mensen je vragen hun gegevens te corrigeren of te verwijderen kun je dit register nodig hebben. Geef deze verzoeken ook door aan de organisaties waarmee je de persoonsgegevens hebt gedeeld.

7. **Heb je de juiste maatregelen genomen om persoonsgegevens te beveiligen?**
   In de AVG staat dat je persoonsgegevens goed moet beveiligen. Bepaal welke technische en organisatorische maatregelen nodig zijn om ervoor te zorgen dat de verwerkingen goed beveiligd zijn. Zo zorg je voor een digitaal veilig bedrijf.

8. **Heb je de vereiste overeenkomsten met partijen die persoonsgegevens voor jou verwerken?**
   Zorg voor een goede verwerksovereenkomst met de partij aan wie de gegevensverwerking is uitbesteed. Je moet als ondernemer zeker zijn dat de data die gebruikt wordt veilig is.

9. **Voldoe je aan de informatieplicht?**
   Je klanten hebben veel rechten op het gebied van privacy. Zorg ervoor dat zij gemakkelijk van die rechten gebruik kunnen maken. Maak een privacyverklaring in eenvoudige taal. Zet daarin wat je doet met persoonlijke gegevens. Waarvoor je de gegevens gebruikt. Waarom dat belangrijk is voor je klanten. En hoe lang je de gegevens bewaart. Zorg dat deze verklaring makkelijk te vinden is.

10. **Ben je voorbereid op mensen die hun privacyrechten willen uitoefenen?**
    Gebruikers (zoals je klanten) hebben zeggenschap over hun gegevens en wat bedrijven daar mee doen. Je klant kan bijvoorbeeld inzage vragen in opgeslagen data of verleende toestemming intrekken. Bereid je organisatie hierop voor. Klanten die denken dat hun

persoonsgegevens op een manier worden verwerkt die in strijd is met de privacywet, kunnen een privacyklacht indienen bij de Autoriteit Persoonsgegevens. De AP kan in zo'n geval onderzoek doen naar aanleiding van de klacht. Je kunt een boete krijgen.

2.3 Boete

De AP controleert of bedrijven zich aan de AVG houden. Zij kunnen ook boetes uitdelen. Jouw bedrijf moet voldoen aan de AVG. In Nederland is de Autoriteit Persoonsgegevens (AP) het orgaan dat hierop toezicht houdt en handhaaft. De boetes kunnen oplopen tot maximaal 20 miljoen euro of 4% van je wereldwijde omzet als je je niet houdt aan de nieuwe privacywetgeving. Dat overkwam de Stichting Bureau Krediet Registratie (BKR). De AP heeft aan BKR een boete opgelegd van 830.000 euro. BKR vroeg vanaf mei 2018 een vergoeding voor het digitaal opvragen van persoonsgegevens. Ook konden mensen maar 1 keer per jaar (per post) zonder kosten hun gegevens inzien. Dat mag niet volgens de privacywetgeving. Daarom is een boete opgelegd van 830.000 euro.

Wolfsen noemt een aantal voorbeelden van hoe het niet moet. "Wat ik een duidelijk voorbeeld vind van onzorgvuldig omgaan met persoonsgegevens, is een huisarts die een verzekeraar moest informeren over de ziekte van zijn patiënt. Hij stuurde toen per abuis het hele medische dossier, inclusief die van andere familieleden, naar de verzekeraar. Een ander voorbeeld is een kinderdagverblijf dat in de nieuwsbrief naar de ouders schreef dat een leidster afwezig was wegens een maagverkleining. Dit is privacyinformatie die je als kinderdagverblijf niet hoort te verspreiden."

Als persoonsgegevens ondanks jouw maatregelen toch op straat belanden, ben je verplicht het datalek te melden bij de Autoriteit Persoonsgegevens. In Nederland vervangt de AVG de Wet Bescherming Persoonsgegevens (Wbp).

3. AVG m.b.t. eerste opzet stakeholders

Na een gesprek met de stakeholder(s) blijkt dat er bij de eerste opzet niet echt gebruik is gemaakt van de AVG. Dit was niet haalbaar voor de prototype die ze hebben ontworpen. Na het maken van het prototype was nog niet duidelijk of mensen er ook echt iets mee konden, vandaar dat de regels minder in acht werden genomen. Bij de bouw is er wel nagedacht over een opzet met een access point. Doordat de telefoon met de knuffel koppelt is deze niet meer aan een ander WiFi netwerk gekoppeld. Je kunt dan alleen de knuffel app openen. Alle bestanden staan alleen op de knuffel en via de app kun je de opnames terugluisteren. Zodra de beheerder via de app iets download is deze zelf verantwoordelijk voor de AVG. De bestanden die worden opgeslagen hebben alleen een tijdsaanduiding en dus geen persoonsgegevens. Verder wordt er niets geregistreerd of gemeten.

4. Werkwijze voor het maken van beeld- en/of geluidsopnamen in de beroepspraktijk

Beeld- en/of geluidsopnamen zijn persoonsgegevens in de zin van de AVG. Het gebruiken van opnamemateriaal uit de beroepspraktijk voor opleidings-, professionaliserings- of kwaliteitsverbeteringsdoeleinden is daardoor een vorm van verwerken van persoonsgegevens. Vanzelfsprekend moet er toestemming gevraagd worden aan degenen die opgenomen worden. Voor bijv. een basisschool, middelbare school of kinderopvang geldt dat zij zelf al generieke maatregelen getroffen hebben. Het kan ook zijn dat ze al een standaard proces hebben afgesproken om toestemmingsverklaringen te verzamelen en te registreren. Controleer vooraf daarom bij de begeleider of contactpersoon ter plaatse of en welke maatregelen getroffen zijn, welke betrokkenen (bijv. kinderen of leerlingen) een generieke toestemmingsverklaring hebben afgegeven. De instelling is verantwoordelijk voor het behartigen van de belangen van de betrokkenen, vraag dus ***niet*** zelf om toestemming aan betrokkenen (Hogeschool van Amsterdam, 2019).

Hoe kan dit concreet aangepakt worden?

- **Controleer of verzorg schriftelijke toestemming**
- **Controleer je opnamen**
  Indien alle betrokkenen toestemming hebben gegeven, controleer dan of betrokkenen die geen toestemming hebben gegeven, daadwerkelijk niet op het materiaal voorkomen.
- **Bewaar en deel de opnamen veilig**
- **Vernietig de opnamen tijdig**
  Wanneer je de beelden of opnamen niet meer nodig hebt voor het doel waarvoor je toestemming hebt gevraagd, dan dien je deze zelf te vernietigen. De passende bewaartermijnen hiervoor zijn: 4 weken na registratie bij opnamen voor reflectie; 1 jaar indien de opname direct bewijsmateriaal is bij beoordeling; 7 jaar indien de opname direct bewijsmateriaal is van het bereiken van het eindniveau van de opleiding.

4.1 Noodzakelijke maatregel

Vanuit de Security specialisatie zagen we meteen al een probleem met de website. Deze website maakt gebruik van HTTP i.p.v. HTTPS. Het probleem van het HTTP-protocol is dat het verkeer dat over het netwerk verstuurd wordt, niet versleuteld is. Een kwaadwillend persoon kan dan meekijken en de onversleutelde gegevens misbruiken. HTTPS zorgt ervoor dat webverkeer versleuteld wordt en dus veel minder makkelijk toegankelijk is door een kwaadwillend persoon. Hierbij kun je denken aan een SSL certificaat. Ook is het van belang dat er een sterk wachtwoord wordt gekozen om in te loggen op de VertelKnuffel. 2-factor authenticatie zou eventueel ook nog een extra oplossing kunnen zijn.

5. Literatuurlijst

1. den Breejen, A. (2021, 17 maart). *Privacywetgeving AVG, wat moet je ermee?* Geraadpleegd op 19 maart 2021, van https://www.kvk.nl/advies-en-informatie/wetten-en-regels/privacywetgeving-avg-wat-moet-je-ermee/
2. Autoriteit Persoonsgegevens. (z.d.). *Mag u persoonsgegevens verwerken?* Geraadpleegd op 20 maart 2021, van https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken
3. Hogeschool van Amsterdam. (2019). *Werkwijze voor het maken van beeld- en/of geluidsopnamen in de beroepspraktijk*. Geraadpleegd van https://www.hva.nl/binaries/content/assets/subsites/werkplekleren/werkwijze-beeld-en-geluidsopnamen-foo.pdf?1566216988622