De AVG in 9 stappen

Ontwikkelaars van games hebben veel te maken met persoonsgegevens. Denk bijvoorbeeld aan IP adressen, spelersstatistieken of de gegevens die je van spelers ontvang als ze een account aanmaken. In sommige gevallen zijn deze persoonsgegevens zelfs erg belangrijk om de game en het verdienmodel te perfectioneren. Meten is immers weten.

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (“AVG”) van toepassing. Deze Europese wet bepaalt onder welke voorwaarden je persoonsgegevens mag verzamelen, gebruiken en delen. Overtreding van deze privacyverplichtingen kan ertoe leiden dat er een (hoge) boete wordt opgelegd. Welke stappen moeten nu worden ondernomen om aan de AVG te voldoen?

De zeven pijlers van de AVG

De kern van de AVG is eigenlijk samen te vatten in 7 beginselen:

1. Persoonsgegevens moeten rechtmatig en behoorlijk worden verwerkt. Daarnaast moet je transparant zijn over wat je met persoonsgegevens doet;
2. Als je persoonsgegevens verwerkt, dan moeten deze juist zijn en waar nodig moet je ze dus actualiseren;
3. Je mag alleen persoonsgegevens verwerken als dat nodig is voor te rechtvaardigen doelen die je voldoende hebt omschreven;
4. Je mag niet meer persoonsgegevens verwerken dan noodzakelijk;
5. Je mag persoonsgegevens niet langer bewaren dan noodzakelijk;
6. Je moet passende technische en organisatorische maatregelen nemen om de persoonsgegevens te beschermen;
7. Wees transparant in je gegevensverwerking.

Deze beginselen moeten worden nageleefd bij het verwerken van persoonsgegevens en zijn voor een gedeelte ook weer nader uitgewerkt in de AVG zelf. We behandelen ze hier stap voor stap.

Stap 1: welke persoonsgegevens worden verwerkt?

Als eerste dient te worden nagegaan welke persoonsgegevens er worden verwerkt of in de toekomst zullen worden verwerkt.

Een persoonsgegeven is *alle* informatie over een geïdentificeerde persoon of een persoon die relatief eenvoudig te identificeren is. Voorbeelden zijn een naam, woonadres en een BSN-nummer, maar ook een IP-adres of een user ID.

Vervolgens moet worden nagegaan of deze persoonsgegevens worden verwerkt.
Onder verwerken worden alle bewerkingen van persoonsgegevens verstaan. Denk dus aan het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken, verspreiden, beschikbaar stellen, aligneren, combineren, afschermen, wissen en vernietigen. Bijna alle handelingen met een persoonsgegevens, dus!

Stap 2: is er een grond aanwezig voor verwerking?

Voor alle persoonsgegevens die worden verwerkt moet een verwerkingsgrondslag zijn. Wat als een verwerkingsgrondslag kan worden beschouwd is limitatief opgesomd in de AVG. Hierbij wordt een onderscheid gemaakt tussen gewone persoonsgegevens en bijzondere persoonsgegevens.

Verwerkingsgronden voor gewone persoonsgegevens zijn onder meer:

1. Toestemming van degene van wie de persoonsgegevens worden verwerkt;
2. Noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is;
3. Noodzakelijk voor het voldoen aan een wettelijke verplichting;
4. Noodzakelijk voor de behartiging van gerechtvaardigde belangen (belangenafweging).

Rechtvaardigingsgronden voor bijzondere persoonsgegevens

De AVG kent een strenger regime voor bijzondere persoonsgegevens.

Bijzondere persoonsgegevens zijn bijvoorbeeld persoonsgegevens waaruit ras of etnische afkomst, politieke opvatting, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken. Daarnaast zijn ook genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid en gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid bijzondere persoonsgegevens.

De rechtvaardigingsgronden voor verwerking van die gegevens zijn onder meer:

1. Uitdrukkelijke toestemming van degene van wie de gegevens worden verwerkt;
2. Noodzakelijk voor het uitoefenen van rechten van de verantwoordelijke of betrokkene op het gebied van arbeidsrecht en het socialezekerheids- en socialebeschermingsrecht;
3. De verwerking ziet op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;
4. Noodzakelijk voor een rechtsvordering;
5. Noodzakelijk voor preventieve of arbeidsgeneeskunde, beoordeling van arbeidsgeschiktheid, medische diagnosen, verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsel en –diensten of sociale stelsel en diensten;
6. Noodzakelijk gelet op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden (let op evenredigheid en neem maatregelen om de privacy-impact zoveel mogelijk te beperken).

Zoals blijkt uit beide opsommingen van rechtvaardigingsgronden is de toestemming van degene van wie persoonsgegevens worden verwerkt altijd voldoende. Er worden alleen wel hoge eisen gesteld aan die toestemming. Die moet namelijk gegeven worden uit vrije wil door iemand die geïnformeerd is. De betrokkene moet dus weten dat hij toestemming geeft en waarvoor hij toestemming geeft. Het verstoppen van toestemming in een privacyverklaring is niet toegestaan en het is aan degene die de gegevens verwerkt om aan te tonen dat toestemming is gegeven.

Stap 3: hoe lang worden de gegevens bewaard?

Vervolgens moet worden bepaald hoe lang gegevens worden bewaard. Hierbij geldt dat gegevens niet langer mogen worden bewaard dan noodzakelijk.

Hoe lang gegevens mogen worden bewaard is ook afhankelijk van de reden waarvoor je ze bewaart. Als het bijvoorbeeld is om een overeenkomst te kunnen uitvoeren, dan is het logisch om de gegevens te bewaren zo lang als de overeenkomst voortduurt.

Soms is het lastig om van te voren duidelijk aan te geven hoe lang gegevens worden bewaard. In dat geval zou volstaan kunnen worden met het aangeven van criteria aan de hand waarvan wordt bepaald of persoonsgegevens verwijderd worden of niet.

Veelal worden gegevens verwerkt zolang een overeenkomst loopt of zolang een bepaalde dienst (bijvoorbeeld een game) geleverd wordt en tot twee jaar daarna. Die twee jaar wordt gerechtvaardigd met het oog op bijvoorbeeld eventueel kunnen beantwoorden van vragen en het voorkomen van claims.

Stap 4: passende technische en organisatorische maatregelen nemen

Als persoonsgegevens worden verwerkt dan moeten er passende technische en organisatorische maatregelen worden genomen om de persoonsgegevens te beveiligen.

Technische en organisatorische maatregelen zijn passend indien zij een op het risico afgestemd beveiligingsniveau waarborgen. Hierbij dient rekening te worden gehouden met:

- de stand van de techniek;
- de uitvoeringskosten;
- de aard, omvang en context van de verwerkingen;
- de verwerkingsdoeleinden, en;
- de waarschijnlijkheid en ernst van de risico's voor rechten en vrijheden van personen.

Uitgangspunt is dat bij verwerking van bijzondere persoonsgegevens altijd de zwaarste technische en organisatorische maatregelen worden geëist. Daarbij kan gedacht worden aan versleutelde opslag, tweetrapsauthenticatie en het voldoen aan vooraf vastgestelde normen (zoals ISO-normen).

Enkele voorbeelden van technische en organisatorische maatregelen:

- beperking toegang servers tot specifieke locaties of IP-adressen;
- twee- of drietrapsauthenticatie
- firewall
- TLS technologie voor de overdracht van data
- beperken maximaal aantal foutieve inlogpogingen
- het voorkomen van schadelijke input door gebruikers (*data sanitizing*)
- beveiligingsupdates
- beperken van de duur van inlogsessies
- wachtwoordbeleid
- beveiligen pand (alarmsystemen, toegangsmogelijkheden, camera's)
- beveiligingsbeleid

Stap 5: moeten verwerkingsovereenkomsten worden gesloten?

Het is mogelijk dat je de verwerking van persoonsgegevens gedeeltelijk door een andere partij laat verrichten. Denk bijvoorbeeld aan een hosting provider, support of marketing research. In dat geval kan het mogelijk verplicht zijn dat je een verwerkersovereenkomst sluit met die andere partij. Dat is afhankelijk van de vraag of die partij de persoonsgegevens voor jou verwerkt.

Een verwerkersovereenkomst is een overeenkomst waarin de voorwaarden worden opgenomen waaronder die partij persoonsgegevens voor jou zal verwerken. Hierin zal onder andere bepaald moeten worden dat deze andere partij gehouden is om de AVG na te leven en wat deze partij moet doen bij een datalek. De verantwoordelijkheid blijft namelijk rusten bij jou!

Stap 6: het informeren van de betrokkene (de privacyverklaring)

Als persoonsgegevens worden verwerkt ben je verplicht om de betrokkenen te informeren over de verwerking en welke rechten zij hebben. Dit gebeurt in een zogenaamde privacyverklaring. Let er ook op dat werknemers ook betrokkenen zijn en dus geïnformeerd dienen te worden door middel van een (interne) privacyverklaring.

Dit zijn de gegevens die in een privacyverklaring moeten zijn geregeld:

Bij persoonsgegevens die je van de betrokkene zelf hebt verkregen:

1.1. Identiteit en gegevens verantwoordelijke
1.2. Contactgegevens functionaris gegevensbescherming (indien van toepassing)
1.3. Welke gegevens verwerkt worden
1.4. Verwerkingsdoeleinden
  1.4.1. Voor welk doel wordt een bepaald persoonsgegeven verwerkt. Noem ook de wettelijke grondslag voor verwerking (zie hieronder). Is de grondslag het ‘gerechtvaardigd belang’, dan moeten ook de gerechtvaardigde belangen genoemd worden.
  1.4.2. Is het noodzakelijk voor het sluiten van de overeenkomst en zo ja, wat is het gevolg als je de gegevens niet verstrekt?
  1.4.3. Verwerkingsdoeleinden moeten concreet benoemd worden. Algemene doelomschrijvingen (verbeteren klantervaring, beveiliging, marketing, etc.) is niet toereikend.
1.5. Ontvangers of categorieën ontvangers van persoonsgegevens.
1.6. Binnen of buiten EU?
1.7. Hoe lang sla je gegevens op?
  1.7.1. Indien je dat niet weet, met behulp van welke criteria besluit je wanneer je gegevens wel of niet meer opslaat?
1.8. Globaal beschrijven technische en organisatorische beveiligingsmaatregelen (het is nog niet duidelijk of dit punt in de AVG is komen te vervallen. Vooralsnog stellen we voor om het toch op te nemen)
1.9. Rechten van betrokkenen:
  1.9.1. Inzage
  1.9.2. Rectificatie
  1.9.3. Wissen
  1.9.4. Beperking van verwerking
  1.9.5. Bezwaar maken tegen verdere verwerking
  1.9.6. Gegevensoverdraagbaarheid
  1.9.7. Intrekken toestemming zonder terugwerkende kracht
  1.9.8. Klacht indienen bij AP

1.10 Als er geautomatiseerde besluitvorming (o.a. profilering) is moet dit genoemd worden. Geef ook aan waarom het gebruikt wordt (belangen) en wat de verwachte gevolgen zijn.

1.11 Bij meerdere verwerkingsverantwoordelijken: naleven artikel 26 AVG.

Persoonsgegevens over betrokkenen verkregen van derden:
Alles wat hierboven uiteen is gezet en de bron waar de gegevens van zijn verkregen

Stap 7: moet er een privacy impact assessment worden verricht?

De PIA is een proces van het omschrijven van verwerkingen, het vaststellen van de noodzakelijkheid en proportionaliteit van de verwerkingen en om risico's die de verwerkingen hebben voor de rechten en vrijheden van natuurlijke personen, te kunnen beheersen. De PIA is geregeld in artikel 35 van de Algemene Verordening Gegevensbescherming (AVG).

Een PIA is vereist als dit is bepaald door de Autoriteit Persoonsgegevens of als de verwerking van persoonsgegevens een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Stap 8: moet er een functionaris gegevensbescherming worden aangesteld?

In sommige gevallen moet een functionaris voor de gegevensbescherming (FG) binnen jouw organisatie worden aangewezen. Dit is een onafhankelijke expert die toeziet op de naleving van de privacyregels en het privacybeleid. Daarnaast geeft de FG ook advies.

Een FG is verplichting in elk geval waarin:

1. een overheidsinstantie of overheidsorgaan de verwerking verricht, met uitzondering van gerechten bij de uitvoering van hun rechterlijke taken;
2. de verantwoordelijke of verwerker hoofdzakelijk is belast met verwerkingen die regelmatige of stelselmatige observatie op grote schaal van betrokkenen vereisen, of;
3. de verantwoordelijke of verwerker hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van persoonsgegevens of strafrechtelijke veroordelingen en strafbare feiten.

Stap 9: moet er een verwerkingsregister worden bijgehouden?

Ten slotte verplicht de AVG dat sommige organisaties een schriftelijk verwerkingsregister bijhouden. Het register dient een (algemene) omschrijving te bevatten van alle verwerkingsactiviteiten.

Een verwerkingsregister is verplicht als jouw organisatie méér dan 250 werknemers heeft.

Daarnaast is het register verplicht indien:

1. Er bijzondere categorieën van persoonsgegevens worden verwerkt of persoonsgegevens over strafbare feiten of het strafrechtelijk verleden;
2. De verwerking een risico inhoudt voor de rechten en vrijheden van betrokkenen;
3. Er sprake is structurele verwerking (dus niet op incidentele basis).

Waar kan Van Iersel Luchtman bij helpen?

Wij kunnen jou als ontwikkelaar helpen bij het voldoen aan de AVG. Vanzelfsprekend kunnen wij al jouw vragen beantwoorden. Maar denk ook aan het opstellen en beoordelen van privacyverklaringen, verwerkersovereenkomsten, verwerkingsregisters en privacybeleid. Daarnaast verrichten wij ook audits om na te gaan in hoeverre jouw organisatie juridisch gezien voldoet aan de AVG en zijn wij beschikbaar om als functionaris voor de gegevensbescherming op te treden.

Speciaal voor leden van DGA hebben wij twee member deals:

Privacyverklaring ***€ 400 ex btw*** *(normaal € 800+)* *Bij de member deal "privacyverklaring" zorgen wij ervoor dat jouw organisatie de betrokkenen afdoende informeert over de wijze waarop je persoonsgegevens verwerkt. Dat betekent ook dat wij bespreken welke persoonsgegevens worden verzameld of je wilt gaan verzamelen en op welke verwerkingsgrondslag dit mogelijk is*	**Verwerkersovereenkomst** ***€ 400 ex btw*** *(normaal € 800+)* *Bij de member deal "verwerkersovereenkomst" zorgen wij ervoor voor passende afspraken met een partij die voor jouw organisatie persoonsgegevens verwerkt. Vooraf inventariseren we vanzelfsprekend of een dergelijke overeenkomst wel noodzakelijk is.*

Disclaimer

Deze informatiebrochure bevat algemene informatie en is met veel aandacht en zorgvuldigheid geschreven. Juridisch advies is echter altijd maatwerk. Wij adviseren in een voorkomend geval altijd om juridisch advies in te winnen afgestemd op uw situatie.

> **Inge Lakwijk** - i.lakwijk@vil.nl
Finance & Restructuring

> **Pieter van Osch** - p.osch@vil.nl
Competition & Procurement law
Commercial contracting

> **Dewi Harkink** - d.harkink@vil.nl
IP, IT & Privacy

> **René Otto** - r.otto@vil.nl
Labour & Employee participation
Corporate & Enterprise