PRIVACY EN APPS

De knelpunten:

- Wie is de verantwoordelijke (voor welke verwerking)?
- Wat is de grondslag voor de verwerking?
- Hoe wordt (ondubbelzinnige/uitdrukkelijke) toestemming verkregen?
- Hoe wordt (tegelijkertijd) voldaan aan de informatieplicht?
- Waar wordt de privacyverklaring geplaatst?
- Wordt de app door kinderen onder de 16 jaar gebruikt?
- Worden er bijzondere gegevens verwerkt?
- Welke gegevens zijn noodzakelijk voor de werking van de app en worden de gegevens in overeenstemming met het doel gebruikt?
- Welke beveiligingsmaatregelen zijn getroffen bij het ontwerp van de app?
- Worden de gegevens doorgegeven naar een land buiten Europa?
- Hoe wordt omgegaan met bewaartermijnen?

Aanbevelingen & Aandachtspunten:

Verantwoordelijke

- U kunt ervan uitgaan dat degene die de app heeft bedacht en gefinancierd als de verantwoordelijke wordt gezien door toezichthoudende instanties. De verantwoordelijke moet voldoen aan alle verplichtingen van de Wbp, waaronder de informatieplicht. De informatieplicht wordt nageleefd door het plaatsen van een privacystatement, privacy verklaring of privacy policy;
- Het is goed mogelijk dat een app-bouwer mede-verantwoordelijke wordt zodra zijn rol en betrokkenheid groter wordt. Bijvoorbeeld zodra er een hosting- en monitoringservice wordt verleend. Let goed op dat u afspraken maakt over aansprakelijkheid bij verlies van data, beschikbaarheid van data en bij het lekken van data;
- In het algemeen wordt een gebruiker van een app niet gezien als een verantwoordelijke, alhoewel hier vanuit juridisch oogpunt over valt te twisten;
- De ontwikkelaar van het apparaat en de ontwikkelaar van het aanwezige besturingssysteem worden ook als verantwoordelijke gezien.

Grondslag

- De grondslagen voor gerechtvaardigde verwerking van persoonsgegevens zijn limitatief opgesomd in de wet (art 8 Wbp);
- In het algemeen kan er vanuit worden gegaan dat de enige bruikbare grondslag voor de verwerking van persoonsgegevens in een app de ondubbelzinnige toestemming van art 8 sub a Wbp is;
- Denkbaar is dat bij hele simpele apps met enkel een backup functie ook gebruik kan worden gemaakt van art 8 sub f Wbp, een gerechtvaardigd doel. Indien u gebruik wilt maken van deze grondslag is het aan te bevelen om de belangenafweging die u hiervoor moet maken op papier te zetten;
- Zodra bijzondere persoonsgegevens worden gebruikt in een app dan geldt het verbod van art 16 Wbp (denk aan gezondheidsgegevens in app voor specifieke doelgroepen). Verwerking kan dan alleen met uitdrukkelijke toestemming (art 23 Wbp);

- Let op: Onder omstandigheden dient ook te worden voldaan aan het toestemmingsvereiste uit de “Cookiewet”, art 11.7a Telecommunicatiewet.

Het verkrijgen van toestemming en voldoen aan informatieplicht:

- De toestemming dient of ondubbelzinnig (art 8 sub a Wbp) of uitdrukkelijk (art 23 Wbp) of toestemming in de zin van art 11.7a Telecommunicatiewet (cookies) te zijn;
- Deze regels kunnen gelijktijdig van toepassing zijn en hier kan gelijktijdig aan worden voldaan;
- Toestemming moet worden gevraagd vóórdat de app informatie van het apparaat haalt;
- Alle soorten toestemming moeten “geïnformeerde toestemming” zijn, concreet: “vrije, specifieke en op informatie berustende wilsuiting”. De toezichthouder is heel streng op dit punt. Is de informatie (in het privacystatement!) niet compleet, niet juist, niet volledig of niet specifiek genoeg, dan geldt de toestemming niet. Met andere woorden: dan heeft u geen grondslag om de gegevens te gebruiken en is uw gebruik onrechtmatig;
- De gebruiker/consument wordt geïnformeerd door een duidelijk, toegankelijk en begrijpelijk privacystatement met duidelijke en begrijpelijke doelen. Wijzig de doelen niet tussentijds;
- Besteed aandacht aan het opstellen van het privacy statement/de privacy policy, dit is maatwerk. De privacy policy is nodig voor het verkrijgen van de geïnformeerde toestemming, maar ook voor het voldoen aan de informatieplicht;
- Voor ondubbelzinnige toestemming zou kunnen worden volstaan met: i) een duidelijke omschrijving in de App Store/Play Store van de verwerkingen van persoonsgegevens ii) met de vermelding dat door installatie ondubbelzinnig akkoord wordt gegaan met de omschreven verwerking iii) voorzien van een link naar een duidelijk, begrijpelijk privacy statement;
- Voor uitdrukkelijke toestemming is tenminste een verplichte acceptatie van het (begrijpelijke) privacy statement nodig, waarbij ook een cancel mogelijkheid wordt geboden en de app niet wordt geïnstalleerd bij gebruik van de cancel mogelijkheid of bij niet acceptatie van de privacy statement;
- Maak toestemming logbaar, zodat kan worden aangetoond dat toestemming is verkregen;
- Het verdient sterk de aanbeveling om voor de verschillende soorten persoonsgegevens apart toestemming te vragen (granulaire toestemming) bijvoorbeeld voor toegang tot contacten, locatie, foto’s, versturen van berichten. Alleen na toestemming voor gebruik van de soort, wordt deze gebruikt;
- Geef gebruikers de mogelijkheid toestemming in te trekken, de app te de-installeren en alle verzamelde gegevens te verwijderen;
- Verzamel alleen gegevens die echt nodig zijn voor de functionaliteit;
- Let op: verwerken op basis van toestemming wordt onder de AVG moeilijker omdat er strengere eisen gaan gelden voor het verkrijgen van rechtsgeldige toestemming.

Plaatsing privacyverklaring:

- De privacy verklaring of privacy statement/privacy policy is nodig om de “geïnformeerde” toestemming te verkrijgen van de gebruiker/consument van de app;
- De privacy verklaring of privacy statement/privacy policy is ook nodig om te voldoen aan de informatieplicht van art 33 en 34 Wbp;
- In de omschrijving in de App Store / Play Store wordt een link geplaatst naar het toepasselijke privacy statement of privacy beleid;

- Voor uitdrukkelijke toestemming is tenminste een verplichte acceptatie van het (begrijpelijke en compleet qua informatie) privacy statement nodig, waarbij ook een cancel mogelijkheid wordt geboden en de app niet wordt geïnstalleerd bij gebruik van deze mogelijkheid;
- Zorg dat het privacy statement goed toegankelijk is, voor en na installatie van de app. Het privacy statement dient ook benaderbaar te zijn in de app;

Kinderen onder de 16 jaar:

- Volgens art 5 Wbp is in de plaats van toestemming van een minderjarige onder de 16 jaar de toestemming van zijn wettelijk vertegenwoordiger vereist;
- Let op dat deze leeftijd in nationale wetgeving kan verschillen;
- De grondslag voor verwerking van persoonsgegevens in app's is nagenoeg altijd toestemming, dus ga na hoe de toestemming van de ouders (aantoonbaar) kan worden verkregen;
- Vermeld het vereiste van toestemming van ouders in de toelichting bij de app in de App Store / Play Store;
- Laat een leeftijdcheck inbouwen die wordt uitgevoerd vóór het in gebruik nemen van de app;
- Vraag op een passende en controleerbare manier om toestemming van de ouders voordat de app in gebruik wordt genomen;
- Wees hierin creatief, sluit aan bij de functie of doelgroep van de app. Verwerk de toestemmingsvraag als opdracht of taakje. Of voer de leeftijdscheck uit door de betaling van Euro 0,01 door een ouder;
- Verzamel in principe niet via de kinderen persoonsgegevens van familie of vrienden;
- Gebruik geen persoonsgegevens van kinderen voor behavioural advertising doeleinden;
- Schrijf de algemene voorwaarden én privacy statement in voor kinderen begrijpbare taal;
- Het kan geen kwaad om een forum waar kinderen actief zijn real time te moderaten (en dit te beschrijven in het privacy statement);
- Verwerk bij voorkeur geen echte profielfoto's van kinderen en geef ze geen foto-maak-en-verzend mogelijkheid. Indien dit onvermijdelijk is, voeg dan attributen toe (hoed, snor, bril) zodat de kinderen zichzelf moeilijker herkenbaar kunnen maken;
- Ga er vanuit dat toezichthouders gegevens van kinderen als gevoelige gegevens kunnen beschouwen, dus tref extra beveiligingsmaatregelen voor hun gegevens en meldt datalekken direct.

Bijzondere gegevens:

- Bijzondere gegevens zijn volgens de Wbp (art 16) gegevens over: godsdienst, gezondheid, ras, politieke voorkeur, seksuele leven, lidmaatschap van vakvereniging, strafrechtelijke gegevens;
- Let op het vervagend verschil tussen gevoelige gegevens zoals financiële gegevens of locatiegegevens en de bijzondere gegevens zoals benoemd in de Wbp. De Autoriteit Persoonsgegevens vindt beide "soorten" persoonsgevens extra waarborgingen moeten krijgen;
- Let ook op of er enkel door de gebruiker zelf ingevoerde gegevens worden verwerkt of dat er ook gegevens van de mobiel of tablet worden gebruikt (denk aan IMEI code, contacten, browse geschiedenis, foto's en video's), hier kunnen ook bijzondere of gevoelige gegevens tussen zitten;

- Indien er bijzondere gegevens worden verwerkt, dient hoe dan ook (uitdrukkelijke!) toestemming te worden gevraagd aan de gebruiker van de app, omdat de verwerking van bijzondere gegevens anders verboden is;
- Of er bijzondere gegevens worden gebruikt, kan enkel worden nagegaan door overleg met de app bouwer vóór het aanbieden van de app in een app store (iOs of Android);
- Bepaal in de opdrachtbevestiging dat de app bouwer verplicht is om zich bij het bouwen van de app aan de Wbp te houden alsof hij zelf de verantwoordelijke is, of dat de app bouwer tenminste u op actieve wijze ondersteund bij het voldoen aan de Wbp en u informeert over de toegang of gebruik van bijzondere gegevens;
- Ga ook na of de app toegang heeft tot foto's en video's. Het kan zomaar zijn dat onbedoeld ras- of gezondheidsgegevens worden verwerkt.

<u>Dataminimalisatie en doelbinding:</u>

- Een van de verplichtingen uit de Wbp is dataminimalisatie, maar ook de verplichting om de data te gebruiken overeenkomstig het doel waarvoor toestemming is gegeven. Implementeer deze verplichtingen in de app;
- Indien geolocatie gegevens worden gebruikt, zorg dat expliciet (= aparte) toestemming wordt gevraagd voor toegang tijdens het gebruik van de app en dat daarnaast aparte toestemming wordt gevraagd voor toegang als de app niet wordt gebruikt (granulaire toestemming);
- Indien geolocatie gegevens worden gebruikt, zorg er dan voor dat de gebruiker deze functie aan en uit kan zetten;
- Zorg dat een gebruiker zelf kan aangegeven tot welke contacten toegang is toegestaan;
- Zorg dat niet op ieder moment geluid wordt opgenomen of gemonitord. Toegang tot geluid is enkel noodzakelijk om een specifieke functie tíjdens het gebruik van de app te laten werken (stem commando).

<u>Beveiliging:</u>

- De beveiligingsverplichting van de Wbp gaat over organisatorische en technische beveiliging. Bepaal dus eerst of er gebruikersgegevens of zelfs gebruikersprofielen worden opgeslagen. Bepaald vervolgens wie er echt toegang moet hebben tot deze gegevens en ken toegangsrechten toe (organisatorische maatregelen);
- Ga ook na waar de gebruikersprofielen worden opgeslagen. Sluit met iedere partij die toegang heeft tot de gegevens in de app een bewerkersovereenkomst (behalve met de gebruiker van de app). Doe dit vóórdat de app wordt aangeboden aan de App store / Play Store;
- Zorg dat in de bewerkersovereenkomst is geregeld dat u als verantwoordelijke de bewerker mag controleren om te zien of hij ook de (beveiligings)verplichtingen na komt;
- Zorg dat u niet afhankelijk bent van andere (contracts)partijen om toegang tot de gegevens in de app te krijgen. Indien verzocht wordt om data overdracht of het wissen van data dan moet u aan deze verzoeken kunnen voldoen, zonder dat een andere partij u hierin hindert. Maak hier afspraken over;
- Vraag aan de app bouwer wie er toegang heeft tot de gegevens in de app. Maak over het verstrekken van deze informatie duidelijke afspraken met de bouwer (verplichting in opdrachtbevestiging);

- Neem de verplichting op in de bewerkersovereenkomst dat de bewerker jaarlijks een beveiligingsplan aanlevert waarin de externe beveiligingsmaatregelen staan, maar ook de interne (namen van personen die toegang hebben tot de gegevens). Controleer dit beveiligingsplan actief;
- Neem ook de verplichting op dat datalekken per direct worden gemeld aan, besproken met en actief worden behandeld in overleg met u als verantwoordelijke;
- Neem ook de verplichting op dat door de bewerker actief wordt meegewerkt indien een appgebruiker zijn wettelijke bevoegdheden uitoefend (o.a. inzage, verwijdering);
- Neem organisatorische maatregelen in het geval de app een moderator functie of monitoring functie heeft, bijvoorbeeld door een extra geheimhouding overeen te komen met de moderator;
- Zorg voor continuiteit van de app, mocht een bewerker failliet gaan of anderszins haar diensten niet meer verlenen dan moet u hier geen last van hebben.

Doorgifte

- Doorgifte is de wettelijke term voor het verstrekken van persoonsgegevens naar een land buiten de Europese Unie. Dit is niet altijd toegestaan;
- Zorg dat u precies weet wáár de gegevens van de app worden opgeslagen. Dit betekent ook dat u moet nagaan waar de hosting aanbieder de gegevens opslaat en waar de medewerkers van de app bouwer aan nieuwe functionaliteiten werken;
- Ga na of de landen waar de gegevens worden opgeslagen een “passend beschermingsniveau” kennen;
- Let op met Safe Harbor certificaten. Vooralsnog biedt dit geen passend beschermingsniveau. Over de vervanger van Safe Harbor bestaat nog onduidelijkheid, althans het US-EU Privacy Shield is nog niet volledig geaccepteerd;
- Sluit zo nodig overeenkomsten af die de letterlijke en ongewijzigde Standard Contractual Clauses bevatten.

Bewaartermijnen

- Ook voor apps geldt de verplichting dat de gegevens niet langer mogen worden bewaard dan nodig is voor het beoogde doel. Dit betekent dus ook dat zodra een gebruiker de app de-installeert, verwijdert van zijn mobile device, dat u ook de gegevens moet verwijderen (tenzij er een andere verplichting bepaalt dat u ze moet of mag bewaren);
- Let op dat de gegevens ook bij derde partijen en bewerkers tijdig worden verwijderd.