AVG checklist Franchise

(Maart 2024)

Sebastiaan van Wijk
Privacy advocaat
vanwijk@dayonelegal.nl
+31 6 1226 6580

Jan-Willem Kolenbrander
Franchise advocaat
kolenbrander@dayonelegal.nl
+31 6 16 0 66 000

Inleiding

De Algemene Verordening Gegevensbescherming is inmiddels bijna zes jaar van kracht. Iedere onderneming in Nederland heeft er mee te maken en moet op basis van de wet maatregelen treffen om goed met persoonsgegevens om te gaan. Ook de maatschappelijke belangstelling voor 'privacy' neemt steeds verder toe, waarbij eventueel verkeerd handelen grote gevolgen kan hebben voor de reputatie van de desbetreffende onderneming. Het is daarom zaak de regels goed na te leven, zeker nu de Autoriteit Persoonsgegevens steeds actiever boetes uitdeelt in het geval van overtredingen.

Ook bij franchising is een goede omgang met persoonsgegevens zeer belangrijk. Franchise is een samenwerkingsvorm tussen zelfstandige ondernemers waarbij de franchisegever tegen vergoeding het recht verstrekt en de plicht oplegt aan een franchisenemer om zijn onderneming te exploiteren binnen de keten van de franchisegever.

In dergelijke franchiserelaties is voldoende aandacht voor privacy een noodzaak. Niet in de laatste plaats omdat er in franchiserelaties vaak grote hoeveelheden persoonsgegevens worden verzameld én onderling met elkaar worden uitgewisseld. Daarover dienen afspraken te worden gemaakt. Voor franchisegevers kan het verder verstandig zijn om te controleren hoe hun franchisenemers omgaan met persoonsgegevens. Gaat het immers mis bij een enkele franchisenemer op dat gebied, dan kan dit negatief afstralen op de hele franchiseformule.

Maar wat vereist de wet nu eigenlijk van franchisegevers en franchisenemers? Wat voor juridische documentatie is er bijvoorbeeld nodig om 'AVG-compliant' te zijn? In deze checklist zetten wij dit kort op een rijtje.

Wat is de AVG?

De Algemene Verordening Gegevensbescherming (AVG) is een Europese verordening die de regels voor de verwerking van persoonsgegevens in de Europese Unie standaardiseert. De AVG heeft rechtstreekse werking in de lidstaten van de Europese Unie en legt verplichtingen op aan bedrijven en organisaties om zorgvuldig om te gaan met (digitale) persoonsgegevens van betrokkenen, zoals consumenten en werknemers. Deze wet geeft betrokkenen nog meer rechten om op te kunnen treden tegen het gebruik en verwerking van hun persoonsgegevens. In Nederland is de Autoriteit Persoonsgegevens (AP) belast met de handhaving van de AVG.

Wat stelt de AVG verplicht?

Veel ondernemingen zullen doorgaans een privacyverklaring hebben opgesteld. Minder bekend is dat in veel gevallen ook zaken als een verwerkingsregister, een datalekkenregister of een zogeheten Gegevensbeschermingseffectbeoordeling (DPIA) nodig zijn in het kader van de AVG. Ook geldt er in sommige gevallen de verplichting om een Functionaris Gegevensbescherming aan te stellen, die onafhankelijk toezicht moet houden op de toepassing en naleving van de privacyregels.

Zijn deze zaken niet op orde, dan kan de AP overgaan tot handhaving. Daarbij geeft de AP zeker niet altijd eerst een waarschuwing. Fikse boetes behoren tot de mogelijke sancties. Mede afhankelijk van de omvang van de onderneming en de aard van de overtreding varieert dit van enkele duizenden tot honderdduizenden of zelfs miljoenen euro's.

Hieronder zetten wij kort uiteen wat franchisegevers en franchisenemer doorgaans minimaal op grond van de AVG geregeld moeten hebben.

> ! *Grip op persoonsgegevens begint bij het in kaart brengen van gegevensstromen. Breng deze gegevensstromen in kaart en beoordeel op welke manier persoonsgegevens een rol spelen binnen de formule. Alleen zo wordt duidelijk wat er al goed is en wat nog ontbreekt. Let daarbij op dat compliance niet alleen ziet op het juridisch op orde hebben van zaken, maar ook gaat over technische en organisatorische maatregelen, bijvoorbeeld hoe persoonsgegevens worden beveiligd of gedeeld.*

A. Verwerkingsregister

Franchisegevers en franchisenemer zullen in de eerste plaats gegevens verwerken van (potentiële) klanten. Dat kunnen de gegevens van klanten zijn die in een fysieke winkel van een franchisenemer zijn achtergelaten, maar betreft ook de gegevens van klanten die op de webshop van de franchisegever een bestelling hebben gedaan. Een vaak voorkomende situatie is dat de franchisegever of de franchisenemers in het kader van 'direct marketing' gegevens van de klanten opnieuw gebruiken en dus verwerken. Daar stopt het echter niet. Ook personeelsgegevens beheren of het vastleggen van bezoekers van de website is een verwerking onder de AVG.

Alle verwerkingen moeten worden vastgelegd in een zogenoemd 'verwerkingsregister'. Daarin moet onder meer opgenomen worden welke gegevens worden verwerkt, met welk doel dat is, met wie deze persoonsgegevens gedeeld worden en hoelang deze gegevens worden bewaard.

Hoewel de AVG uitzonderingen kent, is in de praktijk vrijwel iedere onderneming verplicht een verwerkingsregister bij te houden. Dus ook franchisegevers en franchisenemers. Alleen organisaties die slechts incidenteel persoonsgegevens verwerken, hebben hiertoe geen verplichting. Dat zal uitzondering zijn, want bijvoorbeeld het bijhouden van een personeelsadministratie kwalificeert volgens de AP al als 'niet-incidenteel' en brengt dus ook een verplichting tot het bijhouden van een register met zich mee.

> ! *Zorg ervoor dat er een verwerkingsregister is en houd deze up-to-date. Leg daarin vast welke persoonsgegevens worden verwerkt, van wie die afkomstig zijn en wat er mee wordt gedaan. Leg daarbij ook vast hoelang de gegevens worden bewaard en of ze met een derde partij worden gedeeld. Vermeld ook de (wettelijke) grondslag. De verplicht op te nemen informatie is vastgelegd in artikel 30 van de AVG.*

B. Externe privacyverklaring

Zodra bekend is welke gegevensstromen er precies binnen de organisatie zijn, is de volgende stap om alle betrokkenen op de juiste manier te informeren. De AVG legt namelijk uitgebreide informatieverplichtingen op. Dit houdt in dat de franchisegever of de franchisenemer de betrokkenen moet informeren over wat deze met hun persoonsgegevens doet en waarom. Een veelgebruikt middel hiervoor is een privacyverklaring op de website, waarin wordt uitgelegd welke persoonsgegevens er worden verzameld en waarom dat gebeurt.

Er worden diverse eisen door de AVG gesteld aan een privacyverklaring. De privacyverklaring moet bijvoorbeeld begrijpelijk en voldoende specifiek zijn. Ook moet de privacyverklaring in een voor de betrokkene begrijpelijke taal worden opgesteld. Dat kan in de praktijk betekenen dat als u (bijvoorbeeld) veel zaken doet in Duitsland of Frankrijk, de privacyverklaring (ook) in het Duits of Frans moet worden opgesteld. Alleen in het Nederlands of Engels kan onvoldoende zijn en tot boetes leiden.[1]

Deze transparantie-eisen zijn streng blijkt uit praktijkgevallen. Zo werd door de AP bijvoorbeeld een miljoenenboete aan Uber opgelegd omdat onder andere de privacyverklaring onvoldoende specifiek was.[2]

> ! *Stel een privacyverklaring op waarin wordt uitgelegd hoe de onderneming met de persoonsgegevens omgaat. Het is aan te bevelen om in de privacyverklaring zo transparant mogelijk te zijn en aan te sluiten bij de daadwerkelijke gang van zaken. Let er ook op dat de AVG franchisegevers en franchisenemers verplicht diverse onderwerpen in de privacyverklaring te bespreken. Deze onderwerpen zijn opgenomen in de artikelen 12, 13, 14 en 15 AVG.*

C. Incidentenregister

Een datalek met persoonsgegevens ligt in het huidige digitale tijdperk (helaas) al snel op de loer. Franchisegevers en franchisenemers doen er dan ook goed aan om hiertegen voldoende (beveiligings-)maatregelen te treffen. Maar, los van dat het verstandig is om data binnen de onderneming goed te beschermen, brengt de AVG hier ook enkele wettelijke verplichtingen met zich mee. Zo dienen bijvoorbeeld incidenten en datalekken geregistreerd te worden in een zogenoemd 'incidentenregister'. Daarin moet onder meer worden vastgelegd wat de inbreuk inhield, wat er met de gegevens is gebeurd en welke maatregelen er na de inbreuk genomen zijn. Ook kleine incidenten moeten verplicht worden vastgelegd. Let er daarbij op dat een 'incident' breed gedefinieerd wordt. Ook een verkeerd geadresseerde e-mail is volgens de AVG een te registreren datalek.

Toezicht op datalekken is extra belangrijk, nu u in beginsel verplicht bent om een datalek binnen 72 uur na ontdekking te melden bij de AP. Deze melding is verplicht, tenzij er

---

[1] https://www.autoriteitpersoonsgegevens.nl/actueel/boete-tiktok-vanwege-schenden-privacy-kinderen
[2] https://www.autoriteitpersoonsgegevens.nl/actueel/uber-krijgt-boete-van-10-miljoen-euro-voor-overtreden-privacyregels

slechts een laag risico voor de betrokkenen is om (bijvoorbeeld) bloot gesteld te worden aan zaken als identiteitsfraude of reputatieschade. Een verkeerd geadresseerde e-mail hoeft bijvoorbeeld niet meldingsplichtig te zijn. Wanneer echter gevoelige gegevens zijn gelekt, of juist informatie op grote schaal, dan moet het datalek altijd gemeld worden. En zijn de gevolgen voor de betrokkenen groot, dan moeten ook zij geïnformeerd worden. De verplichting om te melden ligt bij de verwerkingsverantwoordelijke, ook als er een datalek bij een verwerker heeft plaatsgevonden. Goede afspraken met de verwerker over ondersteuning bij een melding zijn dus van belang.

Heeft u als franchisegever of franchisenemer een datalek gehad en dit ten onrechte niet gemeld bij de AP of de betrokkenen terwijl dat wel had gemoeten? Dan kan de AP een (forse) boete opleggen. Het is dan ook zaak om in het geval van datalekken snel te schakelen.

> ! *Houd in een Incidentenregister alle beveiligingsincidenten bij. Of het nu gaat om een verkeerd geadresseerde e-mail of een gestolen (werk)laptop maakt niet uit. Alles moet geregistreerd worden, maar niet alles hoeft gemeld te worden. Probeer bij het wel of niet doen een objectieve afweging te maken van de risico's voor de betrokken personen.*

D. Verwerkersovereenkomsten

Wanneer een franchisegever of franchisenemer persoonsgegevens aan een derde partij verschaft en deze partij voor hen iets met deze persoonsgegevens doet, moet met deze partij ('de verwerker') van de AVG een verwerkersovereenkomst worden gesloten. De salarisadministratie van personeel is een klassiek voorbeeld van zo'n situatie waarin dit nodig is, want de persoonsgegevens van het personeel worden in dat geval gedeeld met en verwerkt door de salarisadministrateur. Een ander voorbeeld is als de franchisenemers de gegevens van hun klanten verplicht aan de franchisegever moeten verstrekken in het kader van landelijke reclame en marketing. Ook de hostingprovider van de webwinkel van de franchisegever kan een verwerker zijn als er persoonsgegevens worden uitgewisseld. In onder andere deze gevallen moet een verwerkersovereenkomst worden gesloten waarin de verplichtingen tussen partijen over en weer worden vastgelegd.

In franchiserelaties is soms niet direct duidelijk wie de verantwoordelijke is voor de verwerking van de persoonsgegevens en wie de verwerker is. Dat de franchisegever dat is als 'verantwoordelijke voor de franchiseformule' ligt voor de hand, maar uit jurisprudentie blijkt dat de vraag wie uiteindelijk verantwoordelijk is, moet worden beantwoord aan de hand van de praktijksituatie. Dit kan dus niet contractueel worden 'weggeschreven'.[3] En diegene die in de praktijk de verantwoordelijke is – hetzij de franchisegever, hetzij de franchisenemer – dient te voldoen aan de verplichtingen die de AVG stelt.

[3] Zie bijvoorbeeld Gerechtshof Amsterdam 5 december 2023, ECLI:NL:GHAMS:2023:2971

Een uitkomst kan ook zijn dat er sprake is van een gezamenlijke verantwoordelijkheid. Dat betekent dat zowel de franchisegever als de franchisenemers verantwoordelijk zijn in de zin van de AVG. Van gezamenlijke verantwoordelijkheid voor de verwerking van persoonsgegevens zal bijvoorbeeld sprake zijn wanneer zowel de franchisegever als de franchisenemer belang hebben bij de verwerking van de persoonsgegevens en invloed hebben op welke gegevens worden verzameld of hoe ze worden verwerkt. Het is niet noodzakelijk dat de franchisegever en de franchisenemer hierin een gelijk aandeel hebben.

> ! *Ga na of er voor het verwerken van persoonsgegevens derde partijen ingeschakeld worden en wie in voorkomend geval de verwerkingsverantwoordelijke of de verwerker is. Sluit in gevallen waar nodig als verantwoordelijke een verwerkersovereenkomst met de verwerker om zo de rechten en plichten juist te verdelen.*

E. Intern Privacy beleid

Wanneer dit passend is vanwege de verwerkingsactiviteiten, moet er ook een intern privacy beleid worden opgesteld. Om te beoordelen of dit noodzakelijk is, moet worden gekeken naar de aard, de omvang, de context en het doel van de gegevensverwerkingen die worden uitgevoerd.

In franchiserelaties kan het zeer raadzaam zijn om een intern beleid op te stellen. Zo is het voor alle franchisenemers - en eventueel de toezichthouder – duidelijk welke stappen door de franchisegever genomen worden om aan de AVG te voldoen en welke stappen de franchisenemers eveneens moeten zetten. De franchisegever doet op deze manier ook aan kwaliteitsborging door ervoor te zorgen dat alle franchisenemers op dezelfde wijze omgaan met eventuele vraagstukken omtrent privacy.

> ! *Stel altijd een privacy beleid op, ook al is het niet verplicht. Duidelijke interne regels helpen ook bij het voorkomen van incidenten en geven aan geïnteresseerden een goed beeld van hoe u met privacy omgaat. Wees in het document zo concreet mogelijk en laat het aansluiten op uw privacyverklaring.*

F. Gegevensbeschermingseffectbeoordeling (DPIA)

Een mogelijk minder bekende verplichting van de AVG is dat er soms ook een zogenoemde 'gegevensbeschermingseffectbeoordeling' (DPIA) uitgevoerd moet worden voordat een verwerking gestart wordt. In gevallen waarbij een verwerking een hoog risico oplevert, bijvoorbeeld door de aard en omvang van de gegevens, moet de verantwoordelijke deze risicoanalyse voorafgaand opstellen. Een DPIA (of het ontbreken daarvan) betekent overigens niet dat een bepaalde verwerking (on)rechtmatig is. Het is vooral de bedoeling dat hiermee privacy risico's in kaart worden gebracht en op die manier maatregelen kunnen worden genomen om risico's te verkleinen.

Dat een DPIA belangrijk is, blijkt uit het feit dat creditcardbedrijf ICS een forse boete van de Autoriteit Persoonsgegevens opgelegd kreeg wegens het ontbreken van een DPIA.[4] Bij die organisatie werd gevoelige informatie, zoals foto's en ID-bewijzen, verzameld zonder dat voorafgaand was getoetst hoe er met eventuele privacy problemen zou worden omgegaan.

> ! *Voer bij structurele verwerkingen altijd een DPIA uit. Daarmee worden de risico's in kaart gebracht en kunnen al direct maatregelen worden getroffen om incidenten te voorkomen.*

Tot slot

Vaak wordt gedacht dat de AVG veel op het gebied van persoonsgegevens onmogelijk maakt en vooral 'lastig' is. Dat is echter niet het geval. Los van dat er een grondslag moet zijn om een bepaalde handeling te verrichten, begint AVG-compliance ook met het op orde hebben van de juiste documenten en informatie. Is dat het geval, dan bent u al een eind op de goede weg!

Heeft u verdere vragen over deze onderwerpen of heeft u hulp nodig met het inzichtelijk krijgen of u wel voldoet aan de verplichtingen van de AVG? Neem dan contact met ons op!

DayOne Advocaten
Laan van NOI 133-H
2593 BM Den Haag
T. +31 70 363 35 55

[4] https://www.autoriteitpersoonsgegevens.nl/actueel/boete-voor-creditcardbedrijf-ics-na-ontbrekende-risicoanalyse