AVG Deel II:

Stap: 1 Bewustwording

Zorg dat iedereen in uw onderneming bekend is met de nieuwe privacyregels.

Stap 2: Informeren

Privacyverklaring

De privacyverklaring of een verwijzing naar de privacyverklaring moet eenvoudig te vinden zijn, daar waar u om persoonsgegevens vraagt. In de privacyverklaring staan in ieder geval:

- uw bedrijfsgegevens
- het doel van de gegevensvastlegging
- welke gegevens u verzamelt
- aan wie u de gegevens eventueel doorgeeft
- hoe lang u de gegevens bewaart
- uitleg over cookies en de reden van gebruik (bij gebruik van cookies)
- de door u toegepaste beveiliging van de vastgelegde persoonsgegevens
- het recht op inzage, correctie, verwijdering en het meenemen van eigen gegevens (dataportabiliteit)
- het recht op intrekking van verleende toestemming
- het recht om een klacht in te dienen
- Eigen gegevens

Het recht om de eigen gegevens in te zien, te corrigeren en aan te vullen was in de oude privacywetgeving al geregeld. Op verzoek moest u de persoonsgegevens ook al verwijderen. Deze rechten blijven onder de nieuwe wet bestaan. Daar komt het recht op dataportabiliteit bij. U moet ervoor zorgen dat mensen hun gegevens makkelijk kunnen ontvangen en kunnen doorgeven aan een andere organisatie als ze dat willen.

Toestemming

Iedereen krijgt door de AVG meer mogelijkheden om voor zichzelf op te komen. De privacyrechten worden versterkt en uitgebreid. De AVG beschrijft hoe u geldige toestemming van mensen kunt krijgen om de persoonsgegevens te mogen verwerken. Daarvoor is een bewuste handeling van de persoon nodig. U mag bijvoorbeeld het vakje voor toestemming niet alvast aankruisen. De verkregen toestemming moet u kunnen aantonen. Het intrekken van de toestemming moet net zo makkelijk zijn als het geven van toestemming.

Klachten

U moet mensen wijzen op de mogelijkheid om bij de Autoriteit Persoonsgegevens een klacht in te dienen over hoe u met hun persoonsgegevens omgaat.

Stap 3: Verwerkingsregister

De AVG verplicht organisaties om de verwerking van persoonsgegevens bij te houden in een register. Deze verplichting geldt voor vrijwel alle organisaties.
U bent verplicht om met een register te werken waarin u de verwerking van persoonsgegevens bijhoudt, als uw organisatie:
persoonsgegevens verwerkt waarvan de verwerking niet incidenteel is (het komt dus vaker voor), of risicovolle persoonsgegevens verwerkt, zoals gegevens over gezondheid, godsdienst of politieke opvattingen, of meer dan 250 medewerkers heeft.

In de praktijk zullen (vrijwel) alle organisaties verplicht zijn de verwerking van persoonsgegevens in een register bij te houden. Dit omdat binnen een organisatie klanten-, leveranciers- of personeelsbeheer altijd vaker voorkomt.

Inhoud register
In het verwerkingsregister neemt u op welke persoonsgegevens u gebruikt, voor welk doel , waar u ze opslaat en met wie u ze eventueel deelt. Het register kunt u schriftelijk of elektronisch bijhouden.
Als betrokken personen u vragen hun gegevens te corrigeren of te verwijderen kunt u dit register hiervoor nodig hebben. U moet deze verzoeken ook doorgeven aan de organisaties waarmee u de persoonsgegevens hebt gedeeld.

Stap 4: Beoordeling impact met DPIA

Bij het verwerken van gegevens met een hoog privacyrisico is een ‘data protection impact analyse’ (DPIA) verplicht. Met deze gegevensbeschermingseffectbeoordeling brengt u de privacyrisico’s van de verwerking van gegevens in kaart. Blijkt uit de DPIA dat de privacyrisico’s hoog zijn, dan kunt u maatregelen nemen om de risico’s te verkleinen.
Een DPIA moet u in ieder geval uitvoeren als u:

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

Er zijn 9 criteria om te toetsen of u een DPIA moet uitvoeren. De Autoriteit Persoonsgegevens (AP) publiceert op termijn een lijst van gegevensverwerkingen waarvoor een DPIA verplicht is.

Stap 5: Inrichten systemen

Bij het inrichten van uw systemen kunt u technisch al een zorgvuldige omgang met persoonsgegevens afdwingen.
Privacy by design
Vraag geen gegevens op die u niet nodig heeft. Voor de verzending van een e-mailnieuwsbrief heeft u bijvoorbeeld geen woonadres nodig. In de AVG wordt dat privacy by design genoemd.

Privacy by default
Bij het vragen om persoonsgegevens moet de standaardinstelling van uw systemen zo privacyvriendelijk mogelijk zijn. De persoon kan zelf gegevens achterlaten of een actieve handeling verrichten om toestemming te geven (opt-in).

U mag bijvoorbeeld geen (web)formulier gebruiken waarop al een vakje is aangevinkt. Ook mag u niet automatisch informatie naar iemand toezenden, zonder dat diegene daar vooraf toestemming voor heeft gegeven. De standaardinstellingen moeten de privacy van iemand respecteren (privacy by default) totdat de persoon zelf toestemming geeft.

Ondanks alle zorg die aan deze special is besteed blijven vergissingen, onjuistheden en/of onvolkomenheden mogelijk en, mede op grond van het informatieve dan wel signalerende karakter van deze special, kunnen wij, de samenstellers, redactie en uitgever daarvoor geen enkele aansprakelijkheid aanvaarden.

Ons kantoor is ingeschreven in het handelsregister onder nummer 56168195

Ook deze special is een extra service van Kantoor Dinkla & Dinkla Bedrijfsadviseurs B.V.