DE VOS & PARTNERS
ADVOCATEN

Het stappenplan voor de AVG

Vanaf 25 mei 2018 is de nieuwe Algemene Verordening Gegevensbescherming (AVG) van toepassing, en zal er een hoop veranderen voor ondernemers. Het is belangrijk om hierop goed voorbereid te zijn, nu de boetes kunnen oplopen tot 20 miljoen of 4% van de jaaromzet.

De AVG is relevant voor ondernemers die persoonsgegevens hebben opgeslagen of iemand anders opdracht hebben gegeven om deze persoonsgegevens te beheren. Persoonsgegevens zijn alle gegevens over een persoon waarmee u diegene kan identificeren, zoals een naam of een adres. Het doel van de AVG is om de privacy van personen beter te beschermen.

De Vos & Partners Advocaten heeft een stappenplan opgesteld om ondernemers "verordeningsproof" te maken.

Stap 1 – Bewustwording

Wat er gaat veranderen: De AVG zal de huidige privacyregels in belangrijke mate wijzigen. Niet iedere ondernemer zal zich dit (op tijd) realiseren.

Actiepunt: Zorg dat de relevante mensen (zoals toezichthouders en beleidsmakers) binnen uw organisatie op de hoogte zijn van de wijzigingen en maak hen bewust van de impact die deze wijzigingen zullen hebben op uw organisatie. Breng vervolgens in kaart wat de benodigde menskracht en middelen zijn voor de implementatie van de nieuwe privacyregels. De implementatie is meer dan enkel de privacy policy op de website aanpassen, dus begin hier op tijd mee.

Stap 2 – Toestemming

Wat er gaat veranderen: De AVG stelt strengere eisen aan de toestemming van een persoon voor het verwerken van zijn persoonsgegevens. De toestemming moet vrij, specifiek, geïnformeerd, ondubbelzinnig, actief en controleerbaar zijn. Uit zwijgen of niet-handelen mag dus geen toestemming worden afgeleid. Let op, als het persoonsgegevens betreft van een kind jonger dan 16 jaar, is de toestemming van een ouder vereist.

Actiepunt: Evalueer de manier waarop u toestemming vraagt, krijgt en registreert en pas deze wijze indien nodig aan. Zorg ervoor dat betrokkenen actief moeten handelen om de toestemming te verlenen, bijvoorbeeld door een hokje aan te vinken. Vermeld hierbij ook waar zij precies toestemming voor geven. Zorg ervoor dat u de leeftijd van personen kan verifiëren en dat u bij personen jonger dan 16 jaar de toestemming van een ouder krijgt.

Stap 3 – Rechten van betrokkenen

Wat er gaat veranderen: De privacy van personen wordt onder de AVG beter beschermd. Onder de huidige wetgeving hadden zij al het recht om te weten welke persoonsgegevens worden verwerkt en zich hiertegen te verzetten. In aanvulling hierop krijgen zij ook:

- recht op rectificatie;
- recht op gegevenswissing;
- recht op beperkte gegevensverwerking;
- recht op bezwaar tegen verwerking ten behoeve van *direct marketing;*
- recht op voorkoming van geautomatiseerde individuele besluitvorming met inbegrip van *profiling*;
- recht op overdraagbaarheid van gegevens (dataportabiliteit).

Elk verzoek van een persoon zal binnen één maand afgehandeld moeten zijn. In de meeste gevallen kunt u geen kosten in rekening brengen voor het afhandelen van deze verzoeken.

Actiepunt: Beoordeel uw privacy/gegevensbeschermingsprocedures en controleer of deze voldoen aan elk van bovengenoemde mogelijke verzoeken van betrokkenen. Ga na of u binnen de genoemde termijn van één maand de verzoeken kan afhandelen.

Stap 4 – Privacyverklaring

Wat er gaat veranderen: Onder de AVG moeten ondernemers informatie verschaffen aan de persoon van wie zij persoonsgegevens verwerken. Deze informatie is onder de AVG breder dan voorheen. In aanvulling op de bestaande eisen moeten ondernemers nu ook (onder andere) de wettelijke grondslag voor de verwerking, de bewaartermijn en de mogelijkheid om een klacht in te dienen opnemen in hun privacyverklaring. Dit kan met het verzenden van een privacyverklaring.

Actiepunt: Heeft u al een privacyverklaring? Zorg dat dan deze huidige privacyverklaring voldoet aan de nieuwe eisen van de AVG. U moet de privacyverklaring direct bij het verkrijgen van de persoonsgegevens aan de persoon verzenden, of, indien u de persoonsgegevens van iemand anders verkrijgt dan van de persoon zelf, binnen een maand na ontvangst. U moet dan ook in de privacyverklaring vermelden van wie u de gegevens hebt ontvangen.

Stap 5 – Documentatie

Wat er gaat veranderen: Hoe documenteert u de persoonsgegevens die u heeft verkregen? Onder de AVG geldt een documentatieplicht. Dit houdt in dat u te allen tijde moet kunnen aantonen welke persoonsgegevens u verwekt. Ook moeten ondernemers kunnen aantonen hoe zij in overeenstemming met de AVG handelen.

Actiepunt: Ten eerste is het belangrijk om niet meer gegevens van een betrokkene te vragen dan nodig is. Hoe minder gegevens u vraagt, hoe minder gegevens u hoeft te documenteren (zie ook stap 7). U moet het volgende documenteren:

- Voor welk doel u de persoonsgegevens gebruikt. Dit kan bijvoorbeeld zijn omdat een persoon zich heeft geabonneerd op uw nieuwsbrief.
- Waar de persoonsgegevens vandaan komen. U moet documenteren of de persoon de gegevens zelf aan u heeft verstrekt of dat u deze bijvoorbeeld van een andere partij heeft ontvangen.
- Met wie u de persoonsgegevens deelt.

- Hoe lang u de persoonsgegevens gaat bewaren.
- Op basis van welke wettelijke grondslag u de persoonsgegevens verwerkt. Dit kan bijvoorbeeld zijn omdat de persoon u toestemming daarvoor heeft gegeven, of omdat u dit moet doen volgens een wettelijke plicht. Inventariseer alle persoonsgegevens en identificeer en documenteer vervolgens de wettelijke grondslag van elke verwerking.

Stap 6 – Datalekken

Wat er gaat veranderen: Datalekken is het tekortschieten van de beveiliging waardoor persoonsgegevens onbedoeld worden verstrekt aan een andere partij. Dit kan bijvoorbeeld gebeuren omdat u bent gehackt of omdat bepaalde systemen niet goed in elkaar zitten. Onder de AVG zijn de regels voor datalekken aangescherpt. Het is verplicht om datalekken aan de Autoriteit Persoonsgegevens (AP) te melden binnen 72 uur, en in de meeste gevallen ook aan de betrokkene.

Actiepunt: Stel een procedure op voor datalekken zodat het duidelijk is welke stappen genomen moeten worden wanneer er sprake is van (een vermoeden van) datalekken. Deze procedure bevat in ieder geval het documenteren van datalekken.

Stap 7 – Preventie

Wat er gaat veranderen: Om datalekken te voorkomen en de privacy te waarborgen zijn de uitgangspunten *privacy by design* en *privacy by default* geïntroduceerd. *Privacy by design* houdt in dat al bij het ontwerpen van de producten en diensten ervoor wordt gezorgd dat persoonsgegevens voldoende worden beschermd. *Privacy by default* houdt in dat er eerst technische en organisatorische maatregelen moeten worden genomen om ervoor te zorgen dat alleen persoonsgegevens worden verwerkt die nodig zijn voor het doel.

Actiepunt: Zorg ervoor dat gegevensbescherming in het technische ontwerp van systemen wordt ingebouwd en dat ze zo zijn ontworpen en ingericht dat er zo min mogelijk persoonsgegevens worden verwerkt. Dit kan bijvoorbeeld door niet meer gegevens te vragen dan nodig is wanneer iemand zich op uw nieuwsbrief wil abonneren of door op uw website het vakje ‘ik wil aanbiedingen ontvangen’ niet vooraf aan te vinken.

Stap 8 – Derden inschakelen

Wat er gaat veranderen: Schakelt u derden in voor bijvoorbeeld het beheer van uw database? Dan maakt u gebruik van een verwerker en gelden extra regels. De afspraken met uw verwerker moeten worden vastgelegd in een zogenaamde “verwerkersovereenkomst”. Onder de AVG zult u ook afspraken moeten maken over verzoeken van betrokkenen, geheimhouding, controle en audits, aansprakelijkheid, bewaartermijnen, back-up en vernietiging bij beëindiging.

Actiepunt: Check wat u precies uitbesteedt aan derden en ga na of er afspraken zijn gemaakt met deze verwerkers. Zorg dat alle afspraken schriftelijk zijn vastgelegd en dat deze verwerkersovereenkomsten voldoen aan de eisen uit de AVG.

Stap 9 – Extra verplichtingen voor bijzondere organisaties

Wat er gaat veranderen: Voor organisaties met meer dan 250 personen in dienst en voor organisaties die 'bijzondere persoonsgegevens" verwerken gelden extra eisen. Bij bijzondere persoonsgegevens kunt u denken aan medische gegevens van een persoon.

Een organisatie met meer dan 250 personen in dienst is verplicht een Functionaris Gegevensbescherming (FG) aan te wijzen. De FG heeft als taak om de werknemers die persoonsgegevens verwerken te informeren en te adviseren over hun verplichtingen uit hoofde van de AVG en toe te zien op de naleving van de AVG.

Bij het verwerken van bijzondere persoonsgegevens kunnen ondernemers verplicht zijn om de privacy risico's uitgebreid te onderzoeken (dit heet een Privacy Impact Assessment (PIA)). Als uit dit onderzoek blijkt dat er te veel risico's kleven aan het werken ervan, moet de AP worden geraadpleegd.

Actiepunt: Stel een FG aan indien uw organisatie dit verplicht is. Dit kan iemand zijn binnen uw organisatie maar ook iemand daarbuiten. Het is aan te raden om een FG aan te stellen met ervaring op het gebied van privacy wetgeving.

Stap 9 : Bel De Vos & Partners Advocaten

Neem contact op met het privacy team van de Vos & Partners Advocaten om u te adviseren over de verplichtingen die op u rusten en te zorgen dat u aan de voor u geldende verplichtingen voldoet. Wij kunnen u bovendien helpen bij het opstellen of controleren van de door u vereiste overeenkomsten. Vraag naar Els Doornhein (edoornhein@devos.nl) en/of Jasper Hulsebosch (Jhulsebosch@devos.nl)