HR Efficiency Partner
Oog voor zaken en mensen

Aanpak AVG – Theoretische wetgeving, vertaald naar de praktijk

#	Wat moet u doen	Waar kunt u dan aan denken
1	Wees voorbereid	• Hoe informeren we nu vast onze klanten, in deze periode voordat de AVG echt van kracht wordt - Iets op de website zetten? - Nieuwsbrief rondsturen? - Alleen reageren als er vragen komen? • Wat moeten onze medewerkers vertellen als er een klant/relatie naar onze voorbereidingen AVG vraagt? • Wat meld ik mijn medewerkers over hun eigen persoonlijke gegevens?
2	Check uw persoonsgegevens/ inventarisatie. • Schakel uw medewerkers hierbij in! 'Benen op tafel sessie' • Hang een groot vel papier op de muur, gebruik een whiteboard o.i.d. en ga schrijven	• Welke informatie vragen wij van klanten? • Welke informatie vragen wij van onze medewerkers • Hebben wij al die informatie echt nodig, wat is het doel? • Bewaren wij die informatie veilig - digitaal met goede wachtwoorden, firewall, bestand tegen hackers e.d - op papier: deugdelijke kasten, slot waar nodig. • Weten wij exact wie waar bij kan? • Weten wij exact wie in de informatie mag veranderen of bijvoorbeeld alleen maar mag lezen? • Zijn er externe partijen die bij onze informatie kunnen uit hoofde van hun werkzaamheden (bijv. de externe salarisadministrateur, de arbodienst, de boekhouder) • Weten wij dat deze externe partijen ook veilig omgaan met de gegevens van onze medewerkers?
3	Bewustwording medewerkers	• Richtlijnen opstellen voor medewerkers over hoe om te gaan met persoonsdata en aan personen gerelateerde data • Zet al die uitleg ook duidelijk op papier en/of digitaal op gemakkelijk bereikbare plaatsen.
4	Vastleggen welke persoonsdata en aan personen gerelateerde data u echt nodig (blijft) hebben. • Schakel uw medewerkers hier weer bij in!	• Aan de hand van de bevindingen uit punt 2 vaststellen welke gegevens we echt nodig hebben, zowel voor klanten als voor medewerkers. • Bepalen wie bij welke informatie kan komen en bijvoorbeeld nieuwe informatie mag opvoeren en/of mag lezen, aanpassen en verwijderen (bijv.: wie mag bij de personeels-gegevens en wat mag hij/zij daarmee doen) • Wie heeft er welke rechten in een digitaal systeem • Vastleggen waar deze data allemaal opgeslagen wordt (digitaal en fysiek) • Is er informatie die wij nodig hebben en waar we toestemming voor moeten vragen

#	Wat moet u doen	Waar kunt u dan aan denken
5	Ga aanpassingen doen	• Een disclaimer op de website voor klanten/relaties met verklaring wat wij precies doen met de informatie die wij van onze klanten bewaren. • Een soortgelijke verklaring voor de medewerkers met verklaring wat wij doen met hun persoonsgegevens en welke externe partijen daarbij betrokken zijn. Laat medewerkers voor ontvangst tekenen. • Maak wachtwoorden sterker, maak een procedure om wachtwoorden sowieso regelmatig te wijzigen • Overleg met de arbodienst over de ziekmeldingsprocedure, klopt die met de nieuwe wetgeving.
6	Klachtenprocedure	• Zet bijvoorbeeld in de disclaimer wat de klanten/relaties moeten doen als ze een klacht hebben over de aanpak van hun persoonsgegevens. • Hou die procedure eenvoudig zodat een klant ons eerder zal benaderen dan de Autoriteit Persoonsgegevens! • Instrueer de medewerkers wat ze moeten doen met een klant/relatie die klaagt over het privacy beleid.
7	Procedure Datalekken	• Informeer medewerkers wat ze moeten doen als ze vermoeden persoonsgegevens kwijt te zijn; zet het op papier, op het interne digitale netwerk o.i.d.; gemakkelijk bereikbaar • Maak een actieplan: wie moet wat doen als we ontdekken dat we persoonsgegevens van bijv. klanten kwijt zijn. • De Autoriteit Persoonsgegevens moet uiterlijk na 72 uur geïnformeerd worden, dus we hebben wel even de tijd.
8	Functionaris gegevens bescherming benoemen	• Hoewel voor de meeste bedrijven niet verplicht, kan het toch handig zijn om één persoon te benoemen die alle acties rondom privacy coördineert en bewaakt. Die weet waar wat is opgeslagen en daar bijv. een lijst van heeft gemaakt en deze steeds up-to-date houdt.
9	(Laten) opstellen van zgn. bewerkersovereenkomsten met derden die data ter beschikking gesteld krijgen of deze voor u verwerken/ opslaan.	• Boekhouder/accountant • Salarisadministrateur • Arbodienst • Banken • Cloud leveranciers • …..

Algemene toelichting:

Bovenstaande lijst geeft een idee waaraan zoal gedacht kan worden om de informatieverwerking en -opslag van privacygevoelige gegevens te laten voldoen aan de richtlijnen van de AVG en hoe dat opgepakt zou kunnen worden. De lijst pretendeert dus beslist niet compleet te zijn! Elke onderneming heeft immers zijn eigen specifieke kenmerken en bedrijfsgegevens.

De officiële richtlijnen zijn te vinden op de website van de Autoriteit Persoonsgegevens: www.autoriteitpersoonsgegevens.nl.

Aan de andere kant: maak het probleem niet groter dan het is. Gebruik het Gezonde Boeren Verstand en zorg dat iedereen in uw onderneming zich er van bewust is dat persoonsgegevens geen gegevens zijn die 'je zomaar rond laat slingeren of weggeeft'.

Tot slot

Voor vragen kunt u mij altijd bellen of mailen:

06 – 53420328
info@hrep.nl

Angela Smeink