Waar je nu spreekt over een maximale boete van 900.000 euro, spreek je in 2018 over een maximale boete van 20 miljoen euro!

STAPPENPLAN: EENVOUDIG VOLDOEN AAN DE GDPR.

Vanaf 25 mei 2018 zijn alle organisaties in Europa verplicht om bij de verwerking van persoonsgegevens te voldoen aan de General Data Protection Regulation (in Nederland ook wel bekend als de Algemene Verordening Gegevensbescherming). Deze strenge nieuwe wet vervangt de huidige Wet bescherming persoonsgegevens (Wbp). Maar wat gaat er nu allemaal veranderen en waarom is het momenteel zo'n hot item?

Hoge boetes liggen op de loer

Met de komst van de nieuwe wet verandert het begrip 'persoonsgegevens'. Naast bestanden met namen, adressen et cetera, vallen binnenkort ook gegevens gekoppeld aan IP-adressen, MAC-adressen, cookies en dergelijke onder de wet. Dit betekent dat bepaalde werkzaamheden vanaf 2018 veel sneller onder de privacywet gaan vallen. Opletten dus! De boetes voor het niet voldoen aan de wet worden namelijk gigantisch hoog. Waar je eerst sprak over een maximale boete van 900.000 euro, spreek je met de komst van GDPR over een maximale boete van 20 miljoen (!) euro. Een gestructureerde aanpak om deze boete niet in je bezit te krijgen, loont dus zeker de moeite!

Risicomanagement als fundament

Om grote problemen (zoals datalekken) te voorkomen, is het noodzakelijk om in eerste instantie alle risico's in kaart te brengen. Ga eens na wat voor soort bedrijf jullie zijn en met welke privacy risico's jullie te maken hebben. Zodra dit inzichtelijk is, kan je hier ook naar handelen. Denk aan het nemen van beheersmaatregelen. Het is hierbij van belang dat alle relevante informatie rondom een beheersmaatregel geregistreerd wordt. Dus zorg dat het duidelijk is wie er bijvoorbeeld verantwoordelijk is voor de evaluatie en hoe de controle op de effectiviteit van een maatregel eruit ziet.

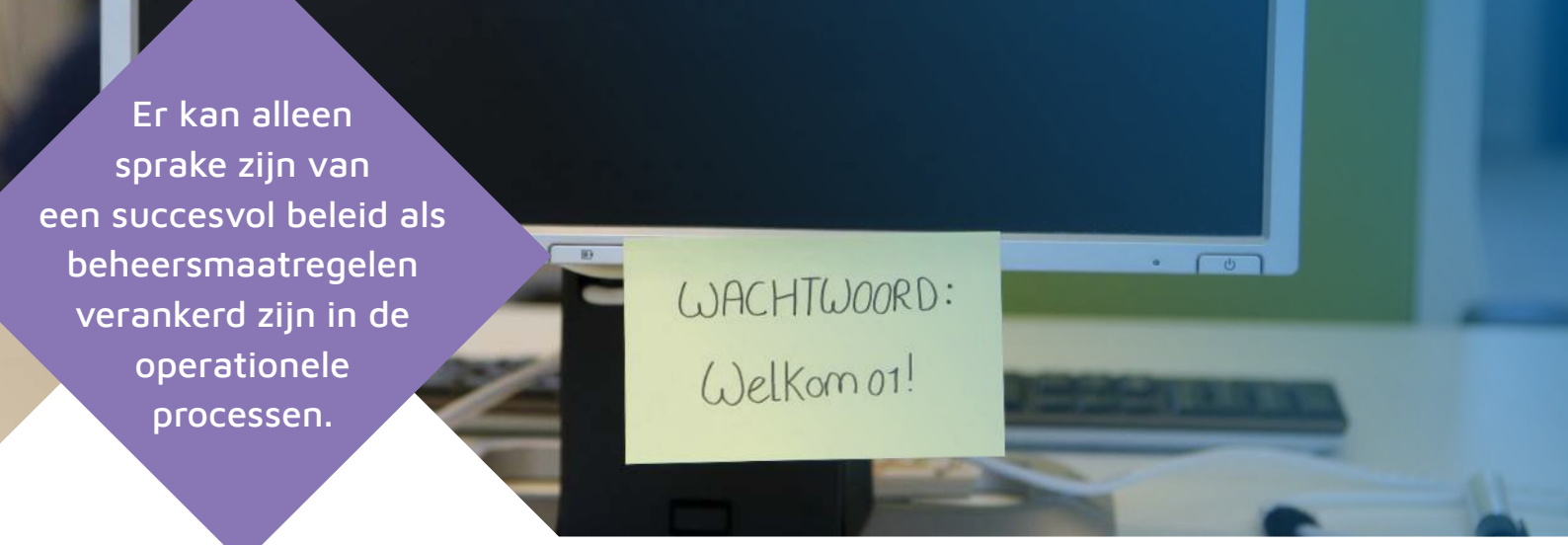
Zorg voor duidelijke processen en verantwoordelijkheden

Er kan alleen sprake zijn van een succesvol beleid en effectieve beheersmaatregelen als deze verankerd zijn in de operationele processen. Leg duidelijk vast wie, waarvoor verantwoordelijk is bij de omgang met persoonsgegevens en wat de bijbehorende taken zijn. Het is hierbij belangrijk dat alle medewerkers hiervan op de hoogte zijn. Ook moeten zij deze informatie eenvoudig kunnen vinden en inzien. Dit is vanaf mei 2018 een verplicht onderdeel van de wet.

Meten = weten

Zodra alles goed is vastgelegd, moeten de afspraken natuurlijk ook worden nageleefd. Maar hoe controleer je of dit daadwerkelijk gebeurt en of beheersmaatregelen voldoende effectief zijn? Periodieke checks en audits kunnen hierbij helpen. Zo maak je niet alleen inzichtelijk OF het beleid wordt nageleefd maar ook HOE het beleid in de praktijk uitpakt. Aan de hand van deze onderzoeksresultaten kunnen verbeterkansen in beeld worden gebracht. Hier kan je vervolgens op inspelen door specifieke acties uit te zetten. Dit continue proces zorgt ervoor dat je als organisatie voortdurend en aantoonbaar verbetert.

De oorzaak van een datalek ligt vaak intern.



Er kan alleen sprake zijn van een succesvol beleid als beheersmaatregelen verankerd zijn in de operationele processen.

Toch gaat het soms mis...

Het kan echter altijd, ondanks alle voorzorgsmaatregelen, gebeuren dat persoonlijke gegevens vrijkomen of onrechtmatig verwerkt worden. Op dat moment heb je te maken met een datalek. Maar wat moet je dan doen? Meld allereerst het datalek intern. De GDPR verplicht je namelijk om alle datalekken te documenteren. Dit in tegenstelling tot de huidige wet. Een datalek melden kan heel eenvoudig en laagdrempelig door gebruik te maken van een meldsysteem. Vervolgens doe je ook een melding bij de toezichthouder (de Autoriteit Persoonsgegevens). Betreft het privacygevoelige data voor opdrachtgevers, dan ben je met de nieuwe wet ook verplicht om dit aan hen te melden. Vervolgens ga je het datalek op een systematische wijze afhandelen en analyseren. Hoe kon dit gebeuren? Deze informatie helpt je vervolgens om het huidige proces te optimaliseren. En denk er vooral ook aan om de geleerde lessen breed te delen binnen de organisatie.

Bewustzijn is de sleutel tot succes

Vaak blijkt uit onderzoek dat de oorzaak van een datalek intern ligt. Hier is een verklaring voor. Medewerkers worden in veel gevallen namelijk te weinig betrokken bij het beleid. Ze worden hier wel over geïnformeerd maar, dit gebeurt nog te vaak middels een standaard nieuwsbrief of een 'saaie' bijeenkomst. Deze manier van informeren komt in 9 van de 10 gevallen gewoonweg niet aan! Het is namelijk te abstract. Je doel is immers niet om mensen te informeren, maar om het bewustzijn te vergroten. Dit kan je doen middels praktische e-learning waarmee je het personeel zelf laat oefenen met situaties waarbij de omgang met persoonsgegevens centraal staat.

Vervolgens kan je het kennisniveau van het personeel testen door leuke, laagdrempelige toetsen uit te zetten. Door met verschillende vraagtechnieken, foto's, video's et cetera te werken, vergroot je de 'fun factor' en automatisch het bewustzijn. Tot slot is dit een ideale manier om ook nieuwe medewerkers snel en eenvoudig te laten beschikken over de benodigde informatie.

Ondersteuning nodig?

Het is nu wel duidelijk waarom deze nieuwe wet zoveel teweeg brengt. De boetes zijn niet alleen gigantisch hoog, het vraagt ook om behoorlijk wat interne aanpassingen en verbeteringen om aan alle verplichtingen te voldoen. Wij begrijpen dat je hier niet op zit te wachten. Niet alleen omdat het veel tijd kost, maar wellicht ook omdat je niet alle kennis of tools in huis hebt om hier zo efficiënt mogelijk op in te spelen. Laat Infoland jou helpen! Middels onze software ondersteunen we je graag bij het opstellen van goede en overzichtelijke risicoprofielen, het actief managen van beheersmaatregelen en het vergroten van het bewustzijn. Hoe wij dit doen? Met de inzet van onze slimme software, genaamd iProva. iProva is een totaaloplossing waarmee wij organisaties (in alle branches) een perfecte ondersteuning bieden op het gebied van risicomanagement, documenten & processen, melden & analyseren, meten & inspecteren en leren & toetsen.

Benieuwd naar de mogelijkheden? Bekijk onze website of neem contact met ons op.

www.infoland.nl
steluwvraag@infoland.nl - 040 848 58 68