White Paper AVG

Voldoet je organisatie al aan de verplichtingen uit de nieuwe wet persoonsgegevens? 25 mei 2018 moet het geregeld zijn in je organisatie!

b2bsure

Voldoet je organisatie al aan de verplichtingen uit de nieuwe wet persoonsgegevens? 25 mei 2018 moet het geregeld zijn in je organisatie!

b2bsure

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Deze wet vervangt de Wet Bescherming Persoonsgegevens. De invoering van de AVG betekent voor jullie organisatie veel aanpassingen op het gebied van processen, IT en legal. De AVG is van toepassing op alle persoonsgegevens, van klanten maar ook van personeel.

Het lastige is dat je uitgewerkt moet hebben waarom je specifieke persoonsgegevens opvraagt. Onderbouw dus waarom je een belang hebt bij het vragen van iemands gegevens. En je moet kunnen laten zien hoe je die toestemming hebt gevraagd. Niet eenmalig maar per handeling. En dat moet je ook nog eens in een intern register bijhouden zodat na te zoeken is waarom je de gegevens hebt opgevraagd en wat je ermee gedaan hebt.

Privacy by design is nu een harde ontwerpeis in de wet. Dat betekent keuzes motiveren waarom het niet een onsje minder kon met die persoonsgegevens die je opvraagt.

En aan de achterkant er ook nog de security. Zorg ervoor dat je kunt aantonen dat je de beveiliging van gegevens op orde hebt. Een virus programma is te weinig! Daarnaast moet je een proces hebben om datalekken proactief op te sporen(!) en te melden indien nodig.

Heel veel zaken rondom privacy moeten worden geregistreerd, allemaal extra administratie. Zaak dus om deze processen vergaand te inventariseren en waar mogelijk te automatiseren.

De invoering van deze wet eist ook nieuwe processen en duidelijke keuzes. Want een simpel registratieformulier in Excel volstaat niet.

Alle stappen die je moet zetten op een rij....

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 je om persoonsgegevens vraagt. In de privacyverklaring staan in ieder geval:

- de bedrijfsgegevens
- het doel van de gegevensvastlegging
- welke gegevens je verzamelt
- aan wie je de gegevens eventueel doorgeeft
- hoe lang je de gegevens bewaart
- uitleg over cookies en de reden van gebruik (bij gebruik van cookies)
- de door je 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 je de persoonsgegevens ook al verwijderen. Deze rechten blijven onder de nieuwe wet bestaan. Je moet ervoor zorgen dat mensen hun gegevens makkelijk kunnen ontvangen en kunnen doorgeven aan een andere organisatie als ze dat willen.

Toestemming

IDe AVG beschrijft hoe je geldige toestemming van mensen kunt krijgen om de persoonsgegevens te mogen verwerken en te verstrekken aan derden. Daarvoor is een bewuste handeling van de persoon nodig. Je moet een vakje laten aankruisen waarin

je toestemming vraagt. De verkregen toestemming moet je vastleggen. En je moet het makkelijk maken de toestemming in te laten trekken.

Klachten

Je moet mensen wijzen op de mogelijkheid om bij de Autoriteit Persoonsgegevens een klacht in te dienen over hoe jouw organisatie 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.

Verplicht gebruik register

Je bent verplicht om met een register te werken waarin je de verwerking van persoonsgegevens bijhoudt, als de 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 neem je op welke persoonsgegevens je gebruikt, voor welk doel, waar je ze opslaat en met wie je ze eventueel deelt.

Als betrokken personen je vragen hun gegevens te corrigeren of te verwijderen kan je dit register daarvoor gebruiken. Je moet deze verzoeken ook doorgeven aan de organisaties waarmee je 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 je de privacyrisico’s van de verwerking van gegevens in kaart. Blijkt uit de DPIA dat de privacyrisico’s hoog zijn, dan moet je maatregelen overwegen om de risico’s te verkleinen.

Verplicht uitvoeren DPIA

Een DPIA moet je in ieder geval uitvoeren als je:

- 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)

DPIA, 9 criteria voor toetsing

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 de systemen kan je deze zo inrichten dat deze een zorgvuldige omgang met persoonsgegevens afdwingt.

Privacy by design

Vraag geen gegevens op die je niet nodig hebt.

Privacy by default

Bij het vragen om persoonsgegevens moet de standaardinstelling van de systemen zo

privacyvriendelijk mogelijk zijn. De persoon kan zelf gegevens achterlaten of toestemming geven (opt-in).

Gebruik geen (web)formulier gebruiken waarop al een vakje is aangevinkt. Ook mag je 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.

STAP 6: Toezicht

Functionaris gegevensbescherming

In bepaalde gevallen is het verplicht om voor uw organisatie een functionaris gegevensbescherming (FG) aan te stellen, ook wel data protection officer (DPO), genoemd. De funtionaris gegevenbescherming is een onafhankelijk persoon die binnen jouw organisatie adviseert en rapporteert over naleving van de AVG.

Aanstelling van een functionaris gegevensbescherming is verplicht wanneer:

- het de kernactiviteit van het bedrijf is om op grote schaal gevoelige persoonsgegevens (zoals gezondheidsgegevens) te verwerken;
- uw organisatie structureel mensen observeert (fysiek of digitaal, bijvoorbeeld via cameraobservatie).

Voor overheidsorganisaties geldt dat de functionaris gegevensbescherming (FG) vrijwel altijd verplicht is.

Intern of extern

De positie functionaris gegevensbescherming kan vanuit de eigen organisatie worden ingevuld, maar de functie kan ook door een externe partij worden vervuld.

Aandacht voor naleving van de AVG is ook van belang voor organisaties die niet verplicht zijn een functionaris gegevensbescherming aan te stellen.

STAP 7: Datalekken documenteren en melden

Een datalek ontstaat als er databestanden worden gehackt of als onbedoeld toegang gegeven is tot bestanden. Ook een gestolen laptop of zoekgeraakte usb-stick is een datalek.

De AVG verplicht je om binnen de organisatie alle datalekken vast te leggen en te documenteren.

Datalek melden

Een datalek moet zo snel mogelijk na ontdekking, zo mogelijk binnen 72 uur, worden gemeld bij de Autoriteit Persoonsgegevens. Deze meldingsplicht geldt niet als er geen risico's voor (natuurlijke) personen uit voortkomen. Wel moet je het datalek intern vastleggen en documenteren. Beschrijft het datalek, de gevolgen van het datalek en de genomen maatregelen.

Datalek bij verwerken data voor anderen

Verwerkt de organisatie privacygevoelige data voor anderen? Dan ben je verplicht het datalek te melden aan de opdrachtgever. De opdrachtgever meldt het zo nodig aan de AP.

STAP 8: Een verwerkersovereenkomst afsluiten

Als een ander bedrijf de persoonsgegevens voor jouw organisatie verwerkt en opslaat, dan moet met dat bedrijf een verwerkersovereenkomst afgesloten worden.

In een verwerkersovereenkomst staat:

- wat het doel en de aard van de verwerking is en welke soort persoonsgegevens worden verwerkt.

En spreek je af:

- dat verwerking uitsluitend plaatsvindt op basis van jouw schriftelijke instructies. Er mogen dus geen persoonsgegevens voor andere doeleinden worden gebruikt;
- personen in dienst van of werkzaam voor de verwerker, een geheimhoudingsplicht hebben;

- de verwerker passende technische en organisatorische maatregelen treft om de verwerking van persoonsgegevens te beveiligen;
- de verwerker zonder schriftelijke toestemming de verwerking niet door een ander mag laten uitvoeren;
- de verwerker helpt om te voldoen aan verzoeken van betrokkenen, als het gaat om hun privacyrechten. Zoals het recht op inzage, correctie, vergetelheid en dataportabiliteit;
- de verwerker helpt om andere verplichtingen na te komen, zoals het melden van datalekken;
- de verwerker na afloop van de verwerkingsdiensten de gegevens verwijdert of terugstuurt. Ook verwijdert hij kopieën, tenzij de verwerker wettelijk verplicht is de gegevens te bewaren;
- de verwerker meewerkt aan audits. Hiervoor stelt de verwerker alle relevante informatie beschikbaar zodat gecontroleerd kan worden of hij zich als verwerker houdt aan de hierboven genoemde verplichtingen.

STAP 9: Leidende toezichthouder bepalen

Als jouw organisatie in meerdere EU-landen actief is, hoef je maar met één privacy toezichthouder (bijvoorbeeld de Autoriteit Persoonsgegevens) zaken te doen, de leidende toezichthouder.

Ben je er klaar voor?

- Bevat ieder (web)formulier een check box, waarbij een persoon bewust een actie moet uitvoeren om akkoord te gaan met het opslaan en verwerken van data?
- Is er een privacy statement aanwezig waarin gedetailleerd, en in jip-en-janneke taal, wordt uitgelegd welke data wordt opgeslagen, waarom, voor hoe lang en hoe de toestemming ingetrokken kan worden?
- Is er per (web)formulier opgeslagen wanneer hij/zij akkoord heeft gegeven en is daarbij ook duidelijk waarop hij/zij akkoord heeft gegeven? Dit geldt ook voor (web)formulieren uit voorgaande jaren.

- Een persoon heeft het recht de over deze persoon opgeslagen gegevens op te vragen. Is je organisatie daarop voorbereid?
- Is een persoon (klant/medewerker) op eenvoudige wijze in staat om zijn/haar voorkeuren te wijzigen?
- Heb je de privacy risico's van alle organisaties, die voor jullie organisatie persoonsgegevens verwerken, in kaart gebracht en voldoen deze "verwerkers" aan de eisen van de AVG?
- Is er, indien nodig, een "functionaris voor gegevensbescherming" (FG) aangesteld?

- **www.b2bsure.nl**