Voldoe in 10 stappen aan AVG

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.

Wat verandert er?
De AVG versterkt de positie van de betrokkenen (de mensen van wie gegevens worden verwerkt). Zij krijgen meer en nieuwe privacy rechten en hun bestaande rechten worden sterker. Organisaties zoals wij en zeer waarschijnlijk ook u, die persoonsgegevens verwerken, krijgen meer verplichtingen.

De nadruk ligt – meer dan nu – op de **verantwoordelijkheid van organisaties om te kunnen aantonen dat zij zich aan de wet houden.**

Dat HLB al ruim twee jaar intensief met privacy en veiligheid bezig is, blijft niet onopgemerkt. De laatste tijd krijgen we regelmatig vragen van klanten over de AVG. Om onze kennis en ervaring te delen en u op weg te helpen hebben we dit AVG-stappenplan uitgewerkt.

Stap 1: Bewustwording

Zorg ervoor dat iedereen in de organisatie (zoals beleidsmakers) op de hoogte zijn van de nieuwe privacyregels. Beleidsmakers moeten kunnen inschatten wat de impact van de AVG is op hun huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen. Iedereen is belangrijk, want iedereen kan persoonlijke gegevens verwerken (zo simpel als een CV opslaan of doorsturen is al een verwerkingsactie!) en verspreiden.

Houd er rekening mee dat de implementatie van de AVG veel kan vragen van de beschikbare menskracht en middelen en het advies is dan ook om er direct mee te beginnen!

Stap 2: Rechten van betrokkenen

Onder de AVG krijgen de mensen van wie persoonsgegevens verwerkt worden meer en verbeterde privacy rechten. Bereid uzelf daar op voor zodat u op tijd en op de juiste manier op verzoeken kunt reageren. Denk daarbij aan bestaande rechten, zoals het recht op inzage en het recht op correctie en verwijdering. Maar houd ook alvast rekening met nieuwe rechten, zoals bijvoorbeeld het recht op dataportabiliteit.

Bij dit recht moet u ervoor zorgen dat betrokkenen hun gegevens makkelijk kunnen krijgen en vervolgens kunnen doorgeven aan een andere organisatie als ze dat willen. Ook kunnen mensen bij de AP (Autoriteit Persoonsgegevens) klachten indienen over de manier waarop er met hun gegevens wordt omgegaan. De AP is verplicht deze klachten vervolgens te behandelen.

Stap 3: Overzicht verwerkingen

Breng uw gegevensverwerkingen in kaart. U moet straks kunnen aantonen welke persoonsgegevens u verwerkt en met welk doel u dit doet, waar deze gegevens vandaan komen en met wie u ze gedeeld heeft.
Onder de AVG heeft de ondernemer zelf een verantwoordingsplicht, wat inhoudt dat u moet kunnen aantonen dat uw organisatie in overeenstemming met de AVG handelt.

U kunt dit overzicht ook nodig hebben als betrokkenen hun privacyrechten willen uitoefenen. Als zij vragen hun gegevens te corrigeren of verwijderen, moet u dit doorgeven aan de organisaties waarmee u hun gegevens heeft gedeeld.

Stap 4: Data protection impact assessment

Onder de AVG kunt u (vooral de grotere partijen onder u) verplicht zijn een zogeheten data protection impact assessment (DPIA) uit te voeren. De DPIA is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Of u een DPIA moet uitvoeren hangt af van een aantal zaken, o.a. bij een hoog privacyrisico (salarisverwerkingskantoren/ uitzendbureaus/ ziekenhuizen, etc) is het verplicht. Controleer dit op de website van de AP!

Mogelijk kan uit een DPIA naar voren komen dat u niet voldoende maatregelen kan treffen voor een veilige verwerking. U bent dan mogelijk verplicht om een voorafgaande raadpleging bij de AP te doen.

Stap 5: Privacy by design & privacy by default

Maak uw organisatie nu al vertrouwd met - de onder de AVG verplichte - uitgangspunten van privacy by design en privacy by default en ga in op hoe ze deze beginselen kunnen invoeren.

Privacy by design houdt in dat er al bij het ontwerpen van producten en diensten zorg gedragen wordt voor de goede bescherming van persoonsgegevens.
Privacy by default houdt in dat technische en organisatorische maatregelen moeten worden genomen om ervoor te zorgen dat u standaard alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken.

Stap 6: Functionaris voor de gegevensbescherming

Onder de AVG kunnen organisaties verplicht zijn om een functionaris voor de gegevensverwerking (FG) aan te stellen. Bedenk nu alvast met de bepalingen en rekenhulp van de AP of dit voor uw organisatie ook geldt.

Stap 7: Meldplicht datalekken

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan de eigen registratie van de datalekken die zich in organisaties hebben voorgedaan. U moet alle datalekken zelf documenteren. Met deze documentatie moet de AP vervolgens kunnen controleren of uw organisatie zich aan deze meldplicht heeft gehouden. Dit gaat veel verder dan de huidige protocolplicht uit de Wbp, die alleen betrekking heeft op de gemelde datalekken.

Kernpunt hierbij blijft dat veel organisaties geen algemeen bekend datalek protocol hebben. Wanneer is die van u gemaakt en/of gecontroleerd?

Stap 8: Bewerkersovereenkomsten

Zijn er gegevensverwerkingen uitbesteed aan een bewerker (in de AVG 'verwerker' genoemd)? Dan zult u een beoordeling moeten maken of de overeengekomen maatregelen in bestaande contracten met hun bewerkers nog steeds toereikend zijn en voldoen aan de vereisten in de AVG. Zo niet, dan zullen er tijdig (!) noodzakelijke wijzigingen moeten worden gedaan.

Stap 9: Leidende toezichthouder

Heeft uw organisatie vestigingen in meerdere EU-lidstaten? Of vinden de gegevensverwerkingen plaats in meerdere lidstaten (denk bijvoorbeeld aan opslag van data via Dropbox/OneDrive/ WeTransfer of het versturen van emails via Gmail). Dan hoeft u onder de AVG nog maar met één privacy toezichthouder zaken te doen. Dit wordt dan de leidende toezichthouder genoemd.

Geldt dit voor u, dan zult u moeten bepalen welke dat gaat worden.

Stap 10: Toestemming

Voor sommige gegevensverwerkingen is toestemming nodig van de betrokkenen. De AVG stelt strengere eisen aan die toestemming. U moet dus goed evalueren op welke manier u hiervoor toestemming vraagt, krijgt en registreert.
Nieuw is dat u ook moet kunnen aantonen dat het een geldige toestemming is (dus dat hij van mensen is gekregen met het doel om persoonsgegevens te verwerken). En dat het voor betrokkenen net zo makkelijk moet zijn om hun toestemming weer in te trekken.

Vragen over de AVG?

Onze adviseurs informeren en adviseren u graag.
Neem contact op met het HLB Privacy Team via avg@hlb.nl.

Lees ook het artikel over de AVG in HLB Nederland Magazine SHIFT #8 (pagina 12),
via **www.hlb.nl/shift**.

HLB Nederland
Accountants & Consultants

www.hlb.nl