

AVG Checklist

01

Op basis hiervan mag je persoonsgegevens verzamelen

Toestemming van de gebruiker

Vitale belangen

Wetterlijke verplichting

Overeenkomst

Algemeen belang

Berechtvaardigd belang

02

Het begint aan de tekentafel

Functionaris gegevensbescherming

Privacy by design

Impact assessment

03

Technische en organisatorische maatregelen

Register met alle verwerkingen

Gegevensbeschermingsbeleid

(Digitale) beveiliging

04

Mensen moeten controle kunnen uitoefenen

Recht om in te zien

Recht om te wijzigen

Recht om vergeten te worden

Recht om gegevens over te dragen

Recht op informatie

AVG Checklist

Bewustwording

Rechten van betrokkenen

Overzicht verwerkingen

Data protection impact assessment

Privacy by design & privacy by default

Functionaris voor de gegevensbescherming

Meldplicht datalekken

Bewerkersovereenkomsten

Leidende toezichthouder

Toestemming

Algemene verordening gegevensbescherming

In 10 stappen voorbereid op de 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?

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 kan ik doen?

Als organisatie kunt u nu alvast stappen ondernemen om straks klaar te zijn voor de AVG. Om u hierbij te helpen, heeft de Autoriteit Persoonsgegevens de 10 belangrijkste stappen voor u op een rijtje gezet. Op autoriteitpersoonsgegevens.nl vindt u de antwoorden op veelgestelde vragen.

AVG Checklist

Bewustwording

Rechten van betrokkenen

Overzicht verwerkingen

Data protection impact assessment

Privacy by design & privacy by default

Functionaris voor de gegevensbescherming

Meldplicht datalekken

Bewerkersovereenkomsten

Leidende toezichthouder

Toestemming

Stap 1

Bewustwording

Zorg ervoor dat de relevante mensen in uw organisatie (zoals beleidsmakers) op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op uw huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen. Houd er rekening mee dat de implementatie van de AVG veel kan vragen van de beschikbare menskracht en middelen en begin er daarom op tijd mee.

De Autoriteit Persoonsgegevens (AP) biedt instrumenten die u kunnen helpen om de AVG na te leven, zoals guidelines die zijn opgesteld samen met de andere privacytoezichthouders in Europa.

Bedenk dat de AP uw organisatie sancties kan opleggen van maximaal 20 miljoen euro of 4% van uw wereldwijde omzet als u zich niet aan de nieuwe privacywetgeving houdt.

AVG Checklist

Bewustwording

Rechten van betrokkenen

Overzicht verwerkingen

Data protection impact assessment

Privacy by design & privacy by default

Functionaris voor de gegevensbescherming

Meldplicht datalekken

Bewerkersovereenkomsten

Leidende toezichthouder

Toestemming

Stap 2

Rechten van betrokkenen

Onder de AVG krijgen de mensen van wie u persoonsgegevens verwerkt meer en verbeterde privacyrechten. Bereid u daar op voor zodat u op tijd en op de juiste manier op verzoeken reageert.

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 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 klachten indienen over de manier waarop u met hun gegevens omgaat. De AP is verplicht deze klachten te behandelen.

AVG Checklist

Bewustwording

Rechten van betrokkenen

Overzicht verwerkingen

Data protection impact assessment

Privacy by design & privacy by default

Functionaris voor de gegevensbescherming

Meldplicht datalekken

Bewerkersovereenkomsten

Leidende toezichthouder

Toestemming

Stap 3

Overzicht verwerkingen

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

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

Vermeld in het overzicht ook per categorie van gegevens op basis van welke wettelijke grondslag u deze gegevens verwerkt. Beroept u zich bijvoorbeeld op een gerechtvaardigd belang of vraagt u toestemming aan de betrokkenen? NB: de grondslagen in de AVG zijn grotendeels hetzelfde als die in de huidige Wbp.

AVG Checklist

Bewustwording

Rechten van betrokkenen

Overzicht verwerkingen

Data protection impact assessment

Privacy by design & privacy by default

Functionaris voor de gegevensbescherming

Meldplicht datalekken

Bewerkersovereenkomsten

Leidende toezichthouder

Toestemming

Stap 4

Data protection impact assessment

Onder de AVG kunt u verplicht zijn een zogeheten data protection impact assessment (DPIA) uit te voeren. Dat 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.

U moet een DPIA uitvoeren als uw beoogde gegevensverwerking waarschijnlijk een hoog privacyrisico met zich meebrengt. U kunt nu alvast inschatten of u straks DPIA's moet uitvoeren en hoe u dit dan gaat aanpakken.

Komt straks uit een DPIA naar voren dat uw beoogde verwerking een hoog risico oplevert? En lukt het u niet om maatregelen te vinden om dit risico te beperken? Dan moet u met de AP overleggen voordat u met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd. De AP beoordeelt dan of de voorgenomen verwerking in strijd is met de AVG. Is dit het geval, dan ontvangt u een schriftelijk advies van de AP.

AVG Checklist

Bewustwording

Rechten van betrokkenen

Overzicht verwerkingen

Data protection impact assessment

Privacy by design & privacy by default

Functionaris voor de gegevensbescherming

Meldplicht datalekken

Bewerkssovereenkomsten

Leidende toezichthouder

Toestemming

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 na hoe u deze beginselen binnen uw organisatie kunt invoeren.

Privacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd.

Privacy by default houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken. Bijvoorbeeld door:

- een app die u aanbiedt niet de locatie van gebruikers te laten registeren als dat niet nodig is;
- op uw website het vakje 'Ja, ik wil aanbiedingen ontvangen' niet vooraf aan te vinken;
- als iemand zich op uw nieuwsbrief wil abonneren niet meer gegevens te vragen dan nodig is.

AVG Checklist

Bewustwording

Rechten van betrokkenen

Overzicht verwerkingen

Data protection impact assessment

Privacy by design & privacy by default

Functionaris voor de gegevensbescherming

Meldplicht datalekken

Bewerkersovereenkomsten

Leidende toezichthouder

Toestemming

Stap 6

Functionaris voor de gegevensbescherming

Onder de AVG kunnen organisaties verplicht zijn om een functionaris voor de gegevensverwerking (FG) aan te stellen. Bepaal nu alvast of dit voor uw organisatie geldt. Zo ja, wacht dan niet te lang met het werven van een FG. Uiteraard mag uw organisatie ook vrijwillig een FG aanstellen.

AVG Checklist

Bewustwording

Rechten van betrokkenen

Overzicht verwerkingen

Data protection impact assessment

Privacy by design & privacy by default

Functionaris voor de gegevensbescherming

Meldplicht datalekken

Bewerkersovereenkomsten

Leidende toezichthouder

Toestemming

Stap 7

Meldplicht datalekken

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

AVG Checklist

Bewustwording

Rechten van betrokkenen

Overzicht verwerkingen

Data protection impact assessment

Privacy by design & privacy by default

Functionaris voor de gegevensbescherming

Meldplicht datalekken

Bewerkersovereenkomsten

Leidende toezichthouder

Toestemming

Stap 8

Bewerkersovereenkomsten

Heeft u uw gegevensverwerking uitbesteed aan een bewerker (in de AVG 'verwerker' genoemd)? Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met uw bewerkers nog steeds toereikend zijn en voldoen aan de vereisten in de AVG. Zo niet, breng dan tijdig noodzakelijke wijzigingen aan.

AVG Checklist

Bewustwording

Rechten van betrokkenen

Overzicht verwerkingen

Data protection impact assessment

Privacy by design & privacy by default

Functionaris voor de gegevensbescherming

Meldplicht datalekken

Bewerkersovereenkomsten

Leidende toezichthouder

Toestemming

Stap 9

Leidende toezichthouder

Heeft uw organisatie vestigingen in meerdere EU-lidstaten? Of hebben uw gegevensverwerkingen in meerdere lidstaten impact? Dan hoeft u onder de AVG nog maar met één privacytoezichthouder zaken te doen. Dit wordt de leidende toezichthouder genoemd. Geldt dit voor uw organisatie, bepaal dan onder welke privacytoezichthouder u valt.

AVG Checklist

Bewustwording

Rechten van betrokkenen

Overzicht verwerkingen

Data protection impact assessment

Privacy by design & privacy by default

Functionaris voor de gegevensbescherming

Meldplicht datalekken

Bewerkersovereenkomsten

Leidende toezichthouder

Toestemming

Stap 10

Toestemming

Voor sommige gegevensverwerkingen hebt u toestemming nodig van de betrokkenen. De AVG stelt strengere eisen aan toestemming. Evalueer daarom de manier waarop u toestemming vraagt, krijgt en registreert. Pas deze wijze indien nodig aan. Nieuw is dat u moet kunnen aantonen dat u geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven.