Charco & Dique

E-paper

Is uw organisatie AVG Proof?

Charco & Dique
020 416 54 03

charcoendique.nl
info@charcoendique.nl

Inleiding

Is uw organisatie AVG Proof?

Privacybescherming is een continu proces dat bijdraagt aan het vertrouwen van mensen in uw organisatie. De Autoriteit Persoonsgegevens heeft een checklist met 10 vragen beschikbaar gesteld die u kan helpen om te toetsen of uw organisatie (nog steeds) aan een aantal belangrijke AVG-verplichtingen voldoet. Hieronder nemen wij deze checklist met u door. Is uw organisatie AVG Proof, of moet u nog actie ondernemen?

Onderwerpen	
1	Heeft u zicht op alle verwerkingen?
2	Heeft u nog steeds een grondslag?
3	Zijn uw (nieuwe) medewerkers privacybewust?
4	Kunnen mensen hun privacyrechten uitoefenen?
5	Is uw overzicht met verwerkingen nog up to date?
6	Moet u een DPIA uitvoeren?
7	Werkt u volgens privacy by design en default?
8	Heeft u een FG of privacycontactpersoon?
9	Kunt u snel handelen bij datalekken?
10	Heeft u grip op uw verwerkers?

1. Heeft u zicht op alle verwerkingen?

Het type gegevens dat uw organisatie verwerkt heeft gevolgen voor de manier waarop u die moet beschermen en aan welke AVG-regels u zich moet houden om AVG Proof te zijn. Bepaalde gegevens zijn door de AVG extra beschermd. Dit zijn bijzondere en strafrechtelijke persoonsgegevens. Voorbeelden van bijzondere gegevens zijn gegevens over de gezondheid of over politieke of religieuze overtuiging.

De verwerking van bijzondere en strafrechtelijke persoonsgegevens is verboden, tenzij u zich kunt beroepen op een specifieke wettelijke uitzondering én op de grondslagen voor het verwerken van 'gewone' persoonsgegevens.

Ook gelden aanvullende eisen voor het verwerken van gegevens van kinderen jonger dan 16 jaar, met name als het gaat om het verkrijgen van toestemming.

Het Burger Service Nummer is volgens de AVG geen bijzonder persoonsgegeven, maar mag alleen worden verwerkt als er een wettelijke basis is.

2. Heeft u nog steeds een grondslag?

U mag alleen persoonsgegevens verwerken wanneer u daarvoor een grondslag heeft. De AVG kent zes grondslagen. Kunt u de gegevensverwerking niet baseren op minimaal een van deze grondslagen? Dan heeft u niet het recht om de persoonsgegevens te verwerken. Ga daarom na of u voor al uw verwerkingen (nog) een grondslag heeft. Het is bijvoorbeeld mogelijk dat een verwerking niet langer 'noodzakelijk is voor de uitvoering van een overeenkomst'. Dan mag u zich niet meer op die grondslag baseren. U bent zelf verantwoordelijk om te beoordelen of u zich voor een verwerking van persoonsgegevens kunt baseren op een van de zes grondslagen:

1. Toestemming van de betrokken persoon.
2. De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst.
3. De gegevensverwerking is noodzakelijk voor het nakomen van een wettelijke verplichting.
4. De gegevensverwerking is noodzakelijk ter bescherming van de vitale belangen.
5. De gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag.
6. De gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen.

3. Zijn uw (nieuwe) medewerkers privacybewust?

Zijn bestaande en nieuwe medewerkers goed op de hoogte van de privacyregels? Zij spelen immers een belangrijke rol in het AVG Proof houden van uw processen, diensten en producten. Zorg er daarom voor dat medewerkers periodiek worden getraind hoe om te gaan met persoonsgegevens en de privacy van uw klanten.

4. Kunnen klanten hun privacyrechten uitoefenen?

Ga na of uw organisatie verzoeken heeft ontvangen van mensen die hun privacyrechten willen uitoefenen en of deze verzoeken volgens de regels zijn afgehandeld. Controleer of uw processen op orde zijn.

De privacyrechten zijn:

- Recht op inzage
- Recht op vergetelheid
- Recht op rectificatie en aanvulling
- Het recht op dataportabiliteit
- Het recht op beperking van de verwerking
- Het recht met betrekking tot geautomatiseerde besluitvorming en profilering.
- Het recht om bezwaar te maken tegen de gegevensverwerking.
- Het recht op duidelijke informatie over wat u met de persoonsgegevens doet.

Ga ook na of uw organisatie zich aan de eigen bewaartermijnen houdt en verwijder gegevens die u niet langer nodig heeft. Op grond van de Algemene verordening gegevensbescherming (AVG) is geen concrete bewaartermijn voor persoonsgegevens vastgesteld. Organisaties bepalen zelf hoe lang zij persoonsgegevens bewaren. Hierbij kijken zij naar hoe lang de gegevens nodig zijn voor het doel waarvoor deze zijn verzameld of worden gebruikt. In andere wetten waar organisaties zich aan moeten houden zijn wel concrete bewaartermijnen vastgesteld, bijvoorbeeld op grond van belastingwetgeving.

5. Is uw overzicht met verwerkingen nog up to date?

Vaak bent u onder de AVG verplicht om een verwerkingsregister bij te houden. Ga in dat geval na of alle (nieuwe) verwerkingen in het verwerkingsregister staan. Of u een verwerkingsregister moet opstellen, hangt af van de omvang van uw organisatie en het type gegevens dat u verwerkt. Het bijhouden van een overzicht van verwerkingen is onderdeel van uw verantwoordingsplicht. In het verwerkingsregister staat informatie over de persoonsgegevens die u verwerkt.

Organisaties met meer dan 250 medewerkers zijn verplicht om een verwerkingsregister bij te houden. Ook organisaties met minder dan 250 medewerkers moeten in de meeste gevallen een verwerkingsregister bijhouden, omdat zij op structurele basis persoonsgegevens van bijvoorbeeld klanten, cliënten, patiënten of inwoners verwerken.
Voor financiële instellingen wordt geadviseerd altijd een verwerkingsregister aan te houden. Hier vindt u een template om uw eigen verwerkingsregister op te stellen

6. Moet u een DPIA uitvoeren?

In sommige gevallen kunt u verplicht zijn om een data protection impact assessment (DPIA) uit te voeren voordat u mag starten met de verwerking. Bij een DPIA worden vooraf de privacyrisico's van een gegevensverwerking in kaart gebracht en maatregelen vastgesteld om de risico's te verkleinen. Ga na of u in de juiste gevallen een DPIA heeft uitgevoerd en of het nodig is voor een eventuele nieuwe verwerkingen waarmee u wilt starten. De AP heeft een lijst van soorten verwerkingen opgesteld waarvoor het uitvoeren van een DPIA verplicht is vóórdat u met verwerken begint. De lijst is niet uitputtend. Het kan zijn dat uw verwerking niet op deze lijst staat. In dat geval moet u zelf beoordelen of uw verwerking een hoog privacyrisico oplevert voor de betrokkenen. Heeft u al eens een DPIA uitgevoerd en aan de hand daarvan maatregelen genomen om bepaalde privacyrisico's te verkleinen? Ga dan na of die maatregelen nog steeds voldoende zijn.

7. Werkt u volgens privacy by design en by default?

Ga na of uw organisatie de verplichte uitgangspunten van privacy by design en privacy by default goed toepast in de praktijk.

Privacy by design houdt in dat u er al bij het (her)ontwerpen van producten en diensten voor zorgt dat persoonsgegevens alleen waar nodig worden opgevraagd, goed worden beschermd en verwijderd wanneer de grondslag voor verwerking vervalt.

Privacy by default betekent dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u 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 registreert als dat niet nodig is;
- op uw website het vakje 'Ja, ik wil aanbiedingen ontvangen' niet vooraf staat aangevinkt;
- als iemand zich op uw nieuwsbrief wil abonneren u niet meer gegevens vraagt dan nodig is.

8. Heeft u een FG of privacycontactpersoon?

Ga na of uw organisatie verplicht is om een functionaris gegevensbescherming (FG) aan te stellen. Zeker wanneer de omvang en activiteiten van uw organisatie zijn veranderd. Organisaties moeten hun FG met een webformulier aanmelden bij de AP. Meldingen die gedaan zijn voor 25 mei 2018 zijn vervallen. Komt u tot de conclusie dat een FG voor u niet verplicht is? Overweeg dan om vrijwillig een privacy contactpersoon aan te stellen, die de privacy aanpak van uw onderneming kan coördineren.

9. Kunt u snel handelen bij datalekken?

Check of u bent voorbereid op een datalek. Vanwege de verantwoordingsplicht moet iedere organisatie die verwerkingsverantwoordelijke is een datalekregister opstellen. In het datalekregister vermeldt de organisatie alle inbreuken die er zijn geweest. Het gaat hierbij zowel om de datalekken die de organisatie moet melden, als datalekken die niet gemeld hoeven te worden.

Ga voor uw organisatie na of zich de afgelopen tijd bijvoorbeeld beveiligingsincidenten hebben voorgedaan? Zo ja, zijn de processen in uw organisatie zo ingericht dat er snel is gehandeld? Zijn datalekken tijdig bij de AP gemeld? En zijn ze goed gedocumenteerd?

Charco & Dique heeft een applicatie die u helpt bij het beoordelen en registreren van datalekken. Hier vindt u de informatie over Sweaper.

10. Heeft u grip op uw verwerkers?

Als u een andere organisatie de opdracht geeft om persoonsgegevens te verwerken waar u zelf verantwoordelijk voor bent, dan bent u de verwerkingsverantwoordelijke en is de andere organisatie de verwerker. U moet dan een verwerkersovereenkomst afsluiten met die andere organisatie. Beoordeel van de bestaande contracten of de met uw verwerkers overeengekomen maatregelen nog steeds toereikend zijn. Controleer ook of de maatregelen in de praktijk worden nageleefd.

Meer weten?
Neem dan contact met ons op.

Bij Charco & Dique beschikken we niet alleen over gedetailleerde kennis van de steeds veranderende financiële wet- en regelgeving, maar hebben we als geen ander de ervaring in huis om onze klanten te ondersteunen bij de toepassing ervan. Soms strategisch, soms pragmatisch maar altijd duurzaam en met vooruitziende blik. Wilt u meer weten over de mogelijkheden? Neem dan contact met ons op.

Neem contact op →

Charco & Dique
020 416 54 03

charcoendique.nl
info@charcoendique.nl