AUTORITEIT
PERSOONSGEGEVENS

Checklist: houd grip op persoonsgegevens

Privacybescherming is een continu proces. En draagt bij aan het vertrouwen van mensen in uw organisatie. Deze checklist helpt u om te toetsen of uw organisatie (nog steeds) aan een aantal belangrijke AVG-verplichtingen voldoet. Zodat u weet of, en zo ja waar, u in actie moet komen.

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.

Ter illustratie: ga bijvoorbeeld na of u niet per ongeluk bijzondere persoonsgegevens verwerkt. Want dat is in de meeste gevallen verboden.

2. Heeft u nog steeds een grondslag?

U mag alleen persoonsgegevens verwerken wanneer u daarvoor een grondslag heeft. Ga daarom na of dat voor al uw verwerkingen zo is.

Ter illustratie: is een verwerking niet langer 'noodzakelijk voor de uitvoering van een overeenkomst'? Dan mag u zich niet meer op die grondslag baseren.

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 privacyproof houden van uw processen, diensten en producten.

Tip: overweeg of het nodig is om (bepaalde) AVG-regels extra onder de aandacht te brengen.

4. Kunnen mensen hun privacyrechten uitoefenen?

Ga na of uw organisatie de afgelopen tijd verzoeken heeft ontvangen van mensen die hun privacyrechten willen uitoefenen. En of die snel en volgens de regels zijn afgehandeld. Zijn uw processen op orde?

Ga ook na of uw organisatie zich aan de eigen bewaartermijnen houdt. Verwijder gegevens die u niet langer nodig heeft.

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.

Het bijhouden van een overzicht van verwerkingen is onderdeel van uw verantwoordingsplicht.

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. Ga na of u dat in de juiste gevallen ook heeft gedaan. En of het nodig is voor eventuele nieuwe verwerkingen waarmee u wilt starten.

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 default?

Past uw organisatie de verplichte uitgangspunten van privacy by design en privacy by default goed toe in de praktijk?

Bijvoorbeeld omdat:
• 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.

Komt u tot de conclusie dat een FG voor u niet verplicht is? Overweeg dan of het kan helpen om vrijwillig een privacycontactpersoon aan te stellen.

9. Kunt u snel handelen bij datalekken?

Check of u bent voorbereid op een datalek. Hebben zich de afgelopen tijd bijvoorbeeld beveiligingsincidenten in uw organisatie 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?

10. Heeft u grip op uw verwerkers?

Heeft u uw gegevensverwerking uitbesteed aan een verwerker? Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met uw verwerkers nog steeds toereikend zijn. En in de praktijk worden nageleefd.

Meer weten over AVG-proof werken?

Deze checklist is een hulpmiddel. Op de website van de AP vindt u meer informatie over deze en andere privacyregels en de antwoorden op veelgestelde vragen.