AUTORITEIT
PERSOONSGEGEVENS

De RvC of RvT en privacy: uw rol als toezichthouder

versie december 2023

Als lid van de raad van commissarissen (RvC) of raad van toezicht (RvT) houdt u de organisatie scherp op tal van vlakken. Daarbij is het belangrijk dat u ook vragen stelt over hoe privacy/de bescherming van persoonsgegevens (hierna: privacy) geregeld is in uw organisatie. U bent immers toezichthouder. Met deze handreiking helpt de Autoriteit Persoonsgegevens (AP) u om de juiste vragen te stellen aan de leiding van uw organisatie, die verantwoordelijk is voor de naleving van de privacywetgeving.

Voor wie?

Dit document is gericht op toezichthouders[1] bij organisaties die een functionaris gegevensbescherming (FG) hebben. Maar ook goed te gebruiken als die FG niet wettelijk verplicht is. Dit document is algemeen van opzet en daardoor toepasbaar in iedere sector. U kunt de vragen zelf aanscherpen door rekening te houden met specifieke kenmerken van uw sector en specifieke ontwikkelingen binnen uw sector.

Als toezichthouder is het een van uw taken om toezicht te houden op de risicobeheersing binnen uw organisatie. U weet als geen ander dat risicobeheersing niet statisch is. De laatste jaren bent u geattendeerd op cyberrisico's voor uw organisatie, maar ook privacy behoeft uw aandacht. De Corporate Governance Code concludeert dan ook over privacy (dataprotectie):

> Eveneens verlangt duurzame lange termijn waardecreatie bewustzijn van en anticiperen op ontwikkelingen in nieuwe technologieën en veranderingen in business modellen en daaraan verbonden risico's waaronder cybersecurity, leveranciers- en ketenafhankelijkheden, data protectie en ethisch verantwoorde toepassing van nieuwe technologieën (bijvoorbeeld Responsible AI).[2]

Met deze handreiking laat de AP zien wat u als toezichthouder kunt doen om bij te dragen aan het borgen van privacy binnen uw organisatie. Het is daarbij essentieel dat er een goede privacycultuur aanwezig is. En dat uw klanten, cliënten of patiënten en ook uw medewerkers dit merken. Zij lopen immers privacyrisico's, doordat uw organisatie hun persoonsgegevens verwerkt. Dit vergt een andere denkwijze dan wanneer u uitgaat van de (cyber)risico's voor uw organisatie, maar is hier een logisch vervolg op.

[1] De AP gebruikt in dit document de term 'toezichthouder', maar bedoelt daarmee ook de commissaris.
[2] Zie https://www.mccg.nl/publicaties/codes/2022/12/20/corporate-governance-code-2022, principe 1.1 en 1.2.1.

AUTORITEIT
PERSOONSGEGEVENS

Uw rol als toezichthouder binnen een organisatie: wat kunt u doen?

Maak gebruik van de instrumenten in de Algemene verordening gegevensbescherming (AVG) die al bestaan binnen de organisatie.[3] Wees daarom goed op de hoogte van de in de AVG opgenomen eisen aan intern toezicht. Zo zijn veel organisaties verplicht om een FG te hebben. De FG houdt – net als u – onafhankelijk intern toezicht op privacy en mag geen instructies ontvangen.[4]

De volgende vragen kunnen helpen om het gesprek aan te gaan met de leiding van uw organisatie over hoe de organisatie omgaat met privacy.

Hoofdvraag 1: Geeft de organisatie genoeg invulling aan de FG-plicht?

Een belangrijke rol bij het toezicht op privacy ligt bij de FG. De leiding van de organisatie moet ervoor zorgen dat de FG-functie aantoonbaar werkt. U kunt deze vragen stellen aan de leiding van uw organisatie:

a) Heeft de FG eenvoudig toegang tot het hoogste leidinggevende niveau van de organisatie, wordt de FG vroegtijdig betrokken bij (door)ontwikkeling van producten, diensten en organisatieontwikkelingen en kan de FG onafhankelijk functioneren?
b) Hoe zijn adviezen en oordelen van de FG onderdeel van de besluitvorming, niet alleen procesmatig maar ook inhoudelijk?
c) Heeft de organisatie een goede leercyclus voor incidenten als datalekken ingesteld, welke verbeterpunten zijn geconstateerd, is daaraan opvolging gegeven en is de FG hierbij betrokken?

Tip: Nodig de FG jaarlijks uit bij uw vergadering en reflecteer samen op de genoemde punten.

Hoofdvraag 2: Hoe geeft de organisatie aantoonbaar invulling aan privacy?

Het recht op privacy is een grondrecht. Dit betekent dat uw organisatie goed moet nadenken over de invulling en uitwerking van dat grondrecht bij alles wat de organisatie doet.

U kunt deze vragen stellen aan de leiding van uw organisatie:

a) Strekt de zorg voor medewerkers zich uit tot en met de digitale wereld? En geldt dat ook voor de zorg voor klanten, cliënten of patiënten? Zo ja, waaruit blijkt dit? Is het onderdeel van de intrinsieke motivatie van leiding en medewerkers, onderdeel van de visie en bijvoorbeeld vervat in kernwaarden?
b) Hoe is het proces voor de identificatie en beperking van privacyrisico's, waaronder datalekken, ingericht en gedocumenteerd? Hoe voert de organisatie dit proces uit en hoe wordt daarover gerapporteerd? Dit geldt voor alle persoonsgegevens, maar in het bijzonder voor de specifieke risico's bij:
   - het gebruik van bijzondere persoonsgegevens;
   - het gebruik van strafrechtelijke gegevens;
   - de eventuele inzet van algoritmes en artificiële intelligentie (AI) bij besluitvorming.

[3] Zie https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg.
[4] Zie https://www.autoriteitpersoonsgegevens.nl/uploads/imported/positionering_van_de_fg.pdf.

c) Wordt er binnen de organisatie waar mogelijk gebruik gemaakt van privacy enhancing technologies[5]?
d) Hoe zijn privacyrisico's van uw ketenpartners – zoals toeleveranciers – in beeld gebracht? En is vastgesteld dat de organisatie persoonsgegevens rechtmatig heeft verkregen van en/of geleverd aan ketenpartners?
e) Worden persoonsgegevens buiten de Europese Economische Ruimte (EER) verwerkt, zijn persoonsgegevens in te zien van buiten de EER en zo ja, gebeurt dit op een rechtmatige manier?
f) Hoe transparant communiceert de organisatie over de verwerkingen van persoonsgegevens, bijvoorbeeld in de privacyverklaring en in jaarverslagen?
g) Welke persoonsgegevens verwerkt de organisatie precies? En staat dit juist en volledig beschreven in een actueel verwerkingsregister?
h) Zijn privacyrisico's een onderdeel van de rapportages van de auditcommissie? En gebruikt de auditcommissie daarvoor ook de informatie uit het verslag van de FG?

De AP vertrouwt erop dat u met deze vragen voldoende invulling kunt geven aan uw toezichthoudende taak. Meer informatie over de AVG vindt u op de website van de AP.

[5] Toegevoegd op 6 september 2024.