AUTORITEIT
PERSOONSGEGEVENS

# Privacy in een jaarverslag

versie december 2023

De Autoriteit Persoonsgegevens (AP) krijgt steeds vaker vragen van grotere bedrijven over wat zij extra kunnen doen om zich te verantwoorden, aanvullend op de verplichtingen uit de Algemene verordening gegevensbescherming (AVG). Zij willen graag structureel en periodiek informatie delen over hoe zij binnen hun bedrijf privacy hebben georganiseerd. Om aan deze behoefte tegemoet te komen, heeft de AP deze vrijblijvende handreiking opgesteld.

## Wat staat er in deze handreiking?

In deze handreiking staan elementen die u kunt gebruiken om een privacyparagraaf in uw jaarverslag op te stellen. Met deze elementen geeft u extra transparantie over privacy aan bijvoorbeeld uw potentiële klanten, aandeelhouders en andere geïnteresseerden.

Let op: stelt u een privacyparagraaf op, dan is dit geen vervanging voor de maatregelen voor transparantie en verantwoording die in de AVG staan. Daaraan moet u nog steeds voldoen op de manier die in de AVG staat.

Tip: Pas deze handreiking gerust aan, zodat deze voor uw situatie relevante elementen bevat. Overweeg aanpassingen wel zorgvuldig, zodat u zeker weet dat u meerdere jaren over dezelfde elementen rapporteert.

## Elementen voor een privacyparagraaf

Hierna noemen we 5 elementen die gezamenlijk de bouwstenen vormen voor een privacyparagraaf in een jaarverslag. Verderop volgt een aantal concrete voorbeelden van de verschillende elementen.

### Element 1: visie en ethiek

Hoe u als bedrijf omgaat met privacy, hangt samen met uw visie en ethiek. Net als bijvoorbeeld de omgang met het milieu. Daarom is het een mooie aanvulling als u ook voor het onderwerp privacy een visie en ethische beschouwing formuleert.

### Element 2: ontwikkelingen binnen en buiten het bedrijf

Er zijn altijd ontwikkelingen binnen uw bedrijf die invloed kunnen hebben op uw verwerkingen van persoonsgegevens. Daarnaast werkt u als bedrijf nooit in een vacuüm. Het is daarom de moeite waard om ook te onderzoeken welke ontwikkelingen van buiten uw bedrijf van invloed zijn op uw verwerkingen en op de rechten van betrokkenen (de mensen van wie u persoonsgegevens verwerkt). Bijvoorbeeld juridische ontwikkelingen, technische ontwikkelingen of marktontwikkelingen. In de privacyparagraaf beschrijft u in hoeverre deze ontwikkelingen impact hebben op uw verwerkingen en de rechten van betrokkenen.

### Element 3: terugkijkend

Geef een kwalitatief beeld van hoe volwassen uw bedrijf is als het om privacy gaat. Daarvoor kunt u volwassenheidsmodellen gebruiken, die een score geven nadat u een selfassesment heeft gedaan of een externe audit heeft laten uitvoeren. Daarnaast kan een meer cijfermatige en feitelijke, kwantitatieve beschouwing helpen om een beeld te schetsen van de status van privacy en de bescherming van persoonsgegevens in uw bedrijf.

### Element 4: vooruitkijkend

Welke stappen wilt u zetten om uw bedrijf volwassener te laten worden op het gebied van privacy? Naast een kwalitatief antwoord op deze vraag, kan het van toegevoegde waarde zijn als u een meer cijfermatig, meetbaar doel opstelt voor het waarborgen van privacy in uw bedrijf.

### Element 5: risico's en bedreigingen

Geef inzicht in de privacyrisico's die in uw bedrijf spelen. Dit vergroot de transparantie. Externe belanghebbenden krijgen hierdoor een goed beeld van de risico's en hoe u daarmee omgaat.

# Voorbeelden van de elementen

Hierna verduidelijken we de genoemde elementen met voorbeelden. Neem voor elk element een kwart tot een half A4 de ruimte.

| Aansluiting onderdeel of onderwerp jaarverslag | Voorbeeld van een invulling |
|---|---|
| Visie en ethiek | Visie en ethiek op het gebied van privacy<br>Wij zijn x, een organisatie die vernieuwend en inclusief is. Dat bepaalt ook onze kijk op privacy. We willen alleen informatie van onze klanten als we die echt nodig hebben. Of als klanten zelf informatie aan ons geven. Dat voelt voor ons dan als bruikleen. Wat betekent dat we heel zorgvuldig met de informatie omgaan, want die is immers niet van ons maar van de klant. Willen klanten hun informatie inzien of laten verwijderen? Geen probleem. Wij stellen geen moeilijke vragen en weten precies waar alles staat. We willen het leven van onze klanten leuker maken, wie ze ook zijn of wat ze ook van ons willen. Wil iemand bij ons iets kopen? Dan vragen we niet naar gender. En wil iemand reclamemail van ons ontvangen met persoonlijke aanbevelingen? Dan moet diegene dat zelf aangeven. Standaard doen we dat namelijk niet. Natuurlijk gaan we even netjes om met de persoonsgegevens van onze medewerkers. Al moeten we van hen wat zaken verplicht registreren, bijvoorbeeld voor de afdracht van belastingen. |

| | |
|---|---|
| Ontwikkelingen | Privacyontwikkelingen van binnenuit<br>In eerdere jaarverslagen hebben we aangegeven dat we onze organisatie mondialer willen maken. We hebben daarvoor specifiek gekeken naar de privacyaspecten. Bijvoorbeeld bij land x, waarnaar we veilig persoonsgegevens kunnen doorgeven omdat er voor dit land een adequaatheidsbesluit geldt van de Europese Commissie. Voor doorgifte van persoonsgegevens naar land y hebben we aanvullende maatregelen genomen na de recente uitspraak van de rechter over het niveau van privacybescherming in dit land.<br><br>Privacyontwikkelingen van buitenaf<br>We zien dat onze klanten steeds privacybewuster worden. Dat vinden we een mooie ontwikkeling, die goed past bij onze doelstellingen. Ook kunnen we de privacyvragen van onze klanten goed beantwoorden.<br><br>Juridische ontwikkelingen<br>Binnenkort wordt Wet X gewijzigd. Daardoor mogen wij niet langer het burgerservicenummer (BSN) gebruiken. We hebben daarom een projectplan opgesteld om zeker te weten dat per 1 januari 202x nergens meer een BSN te vinden is in onze verwerkingen en systemen.<br><br>Technische ontwikkelingen<br>We volgen de ontwikkelingen rondom ‘differential privacy’ op de voet. We zien mogelijkheden om dit in te zetten bij onze verwerkingen van persoonsgegevens. We zijn nu aan het testen of dit goed werkt. Met deze techniek verwachten we minder persoonsgegevens te gaan verwerken. |

| | Kwalitatief | Kwantitatief |
|---|---|---|
| Terugkijkend | Vorig jaar zijn we een project gestart om te onderzoeken of we de volwassenheid van onze organisatie op het gebied van privacy kunnen meten en bewaken. We hebben dat gevonden in model X. Dit model kent y niveaus en we staan nu op de x-de trede van de y. We verwachten aan het einde van het jaar op trede x +1 te staan.<br><br>Dit jaar hebben we grote stappen gezet binnen de branche. We hebben constructieve gesprekken gevoerd met de brancheverenigingover het delen van kennis over privacy en gegevensbescherming. | We hebben de vernieuwde versie gelanceerd van ons opleidingsplan om het privacybewustzijn van medewerkers te vergroten. Op 1/x/202x had al 80% van onze medewerkers de bijbehorende training succesvol doorlopen. Dat betekent dat conform onze planning op 1/x/202x alle medewerkers de training succesvol hebben afgerond.<br><br>We hebben dit jaar helaas een datalek gehad dat x klanten trof. Dit leidde echter niet tot grote risico's voor onze klanten, omdat we weinig persoonsgegevens bewaren en we een goed detectiesysteem hebben. |
| Vooruitkijkend | We gaan verder met onze professionalisering op privacygebied, zowel binnen ons eigen bedrijf als binnen de brancheverenigingen.<br><br>Voor verwerking x willen we meer zekerheid dat we voldoen aan de privacywetgeving. Deze verwerking lijkt ons uitermate geschikt voor een AVG-certificaat. We zijn daarom een project gestart om het certificeringstraject in gang te zetten. | We willen aansluiten bij de brancheverenging. In 20xx willen we dan gezamenlijk een aanvraag doen bij de Autoriteit Persoonsgegevens voor goedkeuring van een gedragscode voor de branche.<br><br>Voor het eind van 20xx willen we vier verwerkingen gecertificeerd hebben. |
| Risico's en bedreigingen | We merken dat sommige van onze verwerkers het lastig vinden om aan onze eisen te voldoen. We gaan daarom extra aandacht besteden aan het vinden van goede verwerkers. Lukt dit niet, dan gaan we mogelijk bepaalde verwerkingen weer zelf uitvoeren in plaats van die uit te besteden. | |

# Vraag en antwoord

## Is het verplicht om een privacyparagraaf op te nemen in een jaarverslag?

Nee, niet vanuit de AVG. U bent weliswaar verplicht op grond van de AVG om transparant te zijn over uw gegevensverwerkingen, maar de AVG schrijft geen privacyparagraaf voor.

De privacyparagraaf heeft vooral als doel om belanghebbenden en geïnteresseerden aan het einde van een boekjaar een beeld te geven van hoe privacy binnen uw organisatie geregeld is. Daarnaast biedt de privacyparagraaf u een uitgelezen kans om te schetsen welke vervolgstappen u wilt zetten om privacy binnen uw organisatie te verankeren. Daarom raadt de AP aan om een privacyparagraaf in uw jaarverslag op te nemen. Dit past bijvoorbeeld goed binnen de Monitoring Code Corporate Governance, als u die gebruikt.

## Mag mijn FG de privacyparagraaf schrijven?

Nee. Het is niet de rol of taak van de functionaris gegevensbescherming (FG) om een privacyparagraaf op te stellen. Dat moet de verwerkingsverantwoordelijke doen. Dit is meestal de persoon binnen uw bedrijf die de hoogst verantwoordelijke is. Het is ook niet de taak van de FG om een privacyparagraaf te beoordelen, accorderen of ondertekenen. De FG houdt alleen toezicht op de privacy in uw bedrijf.
Zijn er in uw bedrijf meerdere verwerkingsverantwoordelijken? Of bent u met een of meerdere andere bedrijven gezamenlijk verwerkingsverantwoordelijk? Dan kunt u een samengestelde privacyparagraaf opstellen.

## Moet ik een afschrift van de privacyparagraaf aan de AP sturen?

Nee. De privacyparagraaf is nadrukkelijk niet bedoeld om de AVG-verplichtingen te vervangen die u heeft richting de AP. Heeft de AP informatie van u nodig? Dan zullen wij u zelf benaderen en de informatie opvragen. De privacyparagraaf heeft juist meerwaarde in de contacten tussen u en andere organisaties dan de AP.

## Welke cijfers moet ik opnemen in de privacyparagraaf?

De privacyparagraaf bestaat uit een terugblik op het afgelopen jaar en een vooruitblik op het komende jaar. Besluit u een privacyparagraaf op te nemen in uw jaarverslag, dan raden wij u aan om alvast na te denken over hoe u na afloop van het komende jaar de terugblik wilt invullen.

Het is goed om ook meer meetbare aspecten op te nemen. In de terugblik kunt u bijvoorbeeld het percentage medewerkers vermelden dat een (interne) training over privacy heeft doorlopen, aantallen datalekken, maar ook hoeveel inzageverzoeken u heeft ontvangen of hoeveel controles u heeft uitgevoerd bij verwerkers. Ook kunt u in de literatuur gangbare methoden gebruiken om de volwassenheid van uw organisatie in een score uit te drukken, zoals het Capability Maturity Model of daarvan afgeleide methodieken.

In de vooruitblik kunt u opnemen welke meetbare doelen u heeft voor het komende jaar. Wilt u bijvoorbeeld dat een x percentage van uw medewerkers een bepaalde training heeft doorlopen, een x aantal controles uitvoeren bij uw verwerkers en/of hoger scoren op volwassenheid?