Bestuur Rendement

Dit artikel wordt u aangeboden door Bestuur Rendement

Bestuur Rendement is hét nieuws- en adviesmagazine voor bestuurders van non-profitorganisaties. Het doel van Bestuur Rendement is om de bestuurder te informeren over alle ontwikkelingen op het gebied van het besturen van een organisatie, financiën, fiscaliteit, personeelszaken en marketing. De bestuurder krijgt praktische informatie over deze verschillende aspecten en waar nodig adviezen voor zijn organisatie.

Bestuur Rendement biedt u:

- veel signalerend nieuws over veranderende wet- en regelgeving;
- beknopte artikelen met veel tips die de lezer direct in de dagelijkse praktijk kan gebruiken;
- marktanalyses over relevante onderwerpen voor de bestuurder.
- wekelijkse e-mailservice met het allerlaatste nieuws;
- een aanvulling op de inhoud van elke uitgave met praktische, online tools.

Kijk voor meer informatie of een proefabonnement op **www.rendement.nl/bestuurblad**

© 2020 Rendement Uitgeverij. Alle rechten voorbehouden

Niets uit deze uitgave mag, noch geheel, noch gedeeltelijk, worden overgenomen en/of vermenigvuldigd zonder voorafgaande schriftelijke toestemming van de uitgever. Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden auteur(s), redacteur(en) en uitgever geen aansprakelijkheid voor eventuele fouten en onvolkomenheden, noch voor de gevolgen hiervan.

AANDACHTSPUNTEN VOOR HET AANSTELLEN VAN EEN PRIVACYTEAM

Bewakers houden de wacht over privacy

Om ervoor te zorgen dat uw organisatie zich aan de privacyregels houdt, is vaak veel kennis en kunde nodig. U kunt ervoor kiezen om een privacyteam op te zetten. Zo'n team zorgt ervoor dat uw organisatie de regels goed naleeft. Hoe groter uw organisatie, hoe groter de klus om een goed team samen te stellen met de juiste taakverdeling en leden die over de benodigde competenties beschikken.

Eén van de eerste vragen die u zich kunt stellen als u bestuurder bent van een grote organisatie, is of het privacyteam een zelfstandig bedrijfsonderdeel moet zijn, of deel moet gaan uitmaken van een andere afdeling. De meest logische keuze is om het team onder te brengen bij de IT-afdeling, omdat daar de meeste kennis van gegevensstromen en beveiliging ligt. Een andere optie is om het privacyteam onder de juridische afdeling te laten vallen.

Maar er valt ook veel voor te zeggen om het privacyteam een geheel zelfstandig bedrijfsonderdeel te laten zijn, met leden van verschillende andere afdelingen. Privacybescherming is een breed vakgebied. Er zijn veel disciplines bij nodig en er moeten veel verschillende afdelingen bij betrokken worden, waaronder:

- management en directie;
- juridisch;
- ICT;
- beveiliging;
- HR;
- financiën.

Als het takenpakket uitgebreid is, zijn vaak verschillende mensen met verschillende kennis en kunde vereist, die vaak al werkzaam zijn op andere afdelingen.

Punten van aandacht bij het inrichten van een privacyteam in uw organisatie

Bij het inrichten van privacyteams moet u een aantal onderwerpen duidelijk bespreken en vastleggen. U kunt de hulp inroepen van uw HR-afdeling bij:

- Hiërarchische structuur. Welke beslisstructuur hanteert uw organisatie? Waar ligt het topmanagement op het onderwerp privacybescherming? Ofwel: wie neemt de belangrijke beslissingen rondom het privacybeleid? Bent u dat als bestuurder?
- Taakomschrijving. Elk lid van het privacyteam moet een duidelijke taakomschrijving hebben. Daarin staat onder meer beschreven waarvoor iemand wordt ingeschakeld en bij wie de bevoegdheden en verplichtingen liggen.
- Evaluatie. Elk team heeft als doel het halen van de privacydoelstellingen die aan de privacyvisie verbonden zijn. Er moet duidelijkheid zijn over hoe evaluatie over de bereikte resultaten plaatsvindt. Evalueer tegelijkertijd de effectiviteit van het privacymanagement.
- Dynamiek. Het is onverstandig om het privacymanagement 'in steen te beitelen'. Privacybescherming is een dynamisch proces. Wees dus niet bang om regelmatig aanpassingen te doen. De techniek schrijdt jaarlijks voort, net als de inzichten van zowel werknemers als overige belanghebbenden. Deze veranderingen moet u meenemen in het privacymanagement.
- Betrokkenheid. Hoe zorgt het privacyteam ervoor dat de verschillende partijen betrokken blijven?
- Communicatie. Dit onderwerp is gerelateerd aan het vorige punt: hoe communiceert het team over de privacymissie, -visie en -doelstellingen? Worden de evaluatieresultaten met iedereen gedeeld, of alleen als er een wijziging is in beleid of procedures?
- Kennisopbouw en het behoud ervan. Hoe brengt u de leden van het privacyteam op het juiste competentieniveau en hoe houdt u ze daar? Wat is het gewenste competentieniveau? Is er een verschil in gewenst niveau voor de verschillende functies in het team?

Privacybescherming onderbrengen bij één specifieke afdeling doet geen recht aan deze werknemers en kan ervoor zorgen dat werknemers de taken van deze collega's als minder relevant zien. Bovendien moet de functionaris voor de gegevensbescherming (FG) rechtstreeks verslag doen aan de hoogste leiding. Als de FG deel uitmaakt van het privacyteam dat bij een bepaalde afdeling is ondergebracht, slaat hij als het ware de natuurlijke bedrijfshiërarchie over.

Centraal

Als uw organisatie verdeeld is over meerdere vestigingen, kunt u het privacymanagement centraal of decentraal regelen. Kiest u ervoor om het privacymanagement lokaal te regelen, welke bevoegdheden geeft u de teams dan? Is het centraal geregeld, dan lopen alle privacyzaken langs één team met één eindverantwoordelijke die de boel aanstuurt. Voordeel is dat er duidelijkheid is met één kapitein aan het roer. Maar vaak is dit gecentraliseerde model traag en het doet niet altijd recht aan individuele situaties: om wanorde te voorkomen, worden de regels strikt toegepast.

Decentraal

Bij gedecentraliseerd privacymanagement werken lokale teams aan de privacyregels. Vaak is het mogelijk om meer soepelheid te creëren dan bij een centrale organisatie. Omdat het lokale team de specifieke situatie beter begrijpt, werkt het eerder naar de geest dan naar de letter van de regels. Is uw organisatie een multinational, dan maakt decentralisatie het eenvoudiger om nationale wetgeving goed in de organisatie in te bedden. De lijntjes zijn vaak korter, waardoor teams beslissingen sneller kunnen nemen. Een groot nadeel is dat elke locatie zijn eigen regels kan maken. Er kunnen botsingen ontstaan tussen verschillende inzichten.

Hybride

Het is allemaal niet zo zwartwit als het gaat om privacymanagement en u hoeft niet te kiezen voor centraal of decentraal als die vormen niet goed bij uw organisatie passen. Er is namelijk ook een 'hybride' variant mogelijk: een mengeling van centraal en decentraal geregeld privacymanagement. Hierbij stelt het hoofdteam op één locatie het beleid en de doelstellingen op en neemt het de uiteindelijke beslissing bij onderlinge conflicten. Binnen vastgestelde grenzen kunnen lokale privacyteams een bepaalde mate van vrijheid gebruiken om recht te doen aan de plaatselijke omstandigheden. U kunt daar een lokale 'privacy officer' aanstellen. Hij legt voor het team verantwoording af aan het lokale management

U kunt ook kiezen voor een mengvorm van centraal en decentraal

en tegelijkertijd ook aan het hoofd van de privacy officers op centraal niveau.

Uitdaging

Het kan een uitdaging zijn om een mengeling van centraal en decentraal geregeld privacymanagement te implementeren. Zo moet u waken voor een te strenge regelgeving vanuit het hoofdkantoor. Ook moeten er duidelijke regels komen voor de inspraak vanuit de verschillende onderdelen. Het gevaar bestaat namelijk dat de ene lokale afdeling meer invloed gaat uitoefenen op het hoofdkantoor dan de andere, waardoor de relatie met verschillende partijen kan scheefgroeien of verslechteren. Een goede methode om genoemde uitdagingen het hoofd te bieden, is om vanuit alle lokale teams één afgevaardigde regelmatig naar het hoofdkantoor te laten komen. De afgevaardigde kan daar zowel individueel als in de groep overleggen met het hoofdteam.

Voordelen

Ondanks de uitdagingen die het opstellen van een hybride team kent, heeft het belangrijke voordelen, namelijk flexibiliteit en lokale variatie. Daarnaast hoeft niet elk team het wiel elke keer opnieuw uit te vinden: het hoofdkantoor kan oplossingen voor vaker voorkomende processen en problemen aandragen bij andere bedrijfsonderdelen of locaties. Nog een ander groot voordeel: werknemers zullen voorstander zijn van de hybride oplossing. Een lokaal privacyteam kan veel meer aandacht besteden aan de plaatselijke omstandigheden. Dat maakt de benadering persoonlijker en specifieker, en creëert daardoor draagvlak op de werkvloer. Uiteraard kan dat er weer toe leiden dat uw organisatie de privacybescherming beter op orde heeft.

Joris Bijvoets, functionaris gegevensbescherming en privacy & security consultant bij AVG Compleet, tel: 020 226 59 03, e-mail: info@avg-compleet.nl

Taken die veel privacyteams op zich nemen

Bij het samenstellen van een privacyteam moet u weloverwogen keuzes maken. Maar omdat iedere organisatie anders is, is het lastig om hier harde richtlijnen voor op te stellen. Wat betreft het takenpakket zijn er wel een aantal taken te noemen die vrijwel elk team zal uitvoeren:

- toezicht houden op de uitvoering van privacyregels;
- bewustwording creëren bij het personeel;
- voorlichting geven;
- adviseren bij nieuwe ontwikkelingen;
- opstellen en evalueren van beleid en procedures rondom privacybescherming;
- implementatie en onderhoud van een Information Security Management System (ISMS);
- controleren of het privacy- en informatiebeveiligingsbeleid wordt nageleefd;
- interne audits uitvoeren.