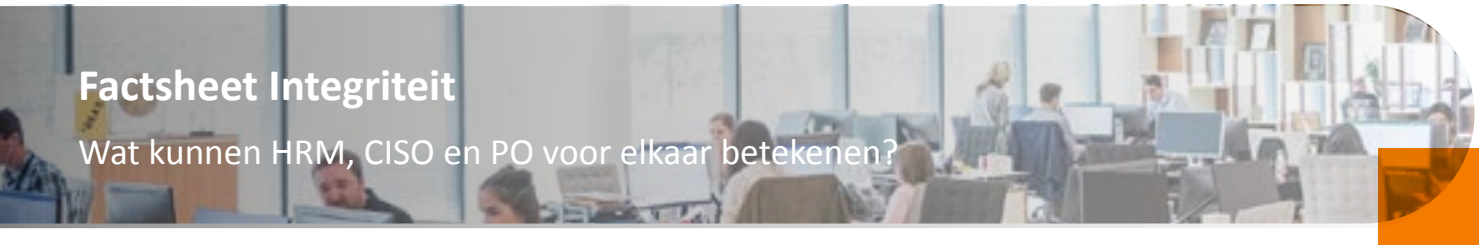
INFORMATIE
BEVEILIGINGS
DIENST



Factsheet Integriteit

Wat kunnen HRM, CISO en PO voor elkaar betekenen?

De medewerk(st)er HRM, de Chief Information Security Officer (CISO) en de Privacy Officer (PO) zijn functies die inhoudelijk van elkaar verschillen. Maar er is een gedeelde zorg, namelijk: hoe bewaken we de integriteit van medewerkers? Samenwerking tussen HRM, CISO en PO om veilig gedrag te bevorderen ligt voor de hand. In deze factsheet schetsen we de wettelijke kaders en doen we suggesties voor de aanpak van integriteitsbevordering.

Versterk elkaar

Vanaf 1 januari 2020 geldt de Wet normalisering rechtspositie ambtenaren (Wnra). Deze wet heeft het nodige veranderd aan de wijze waarop overheden invulling moeten geven aan de regels op het gebied van integriteit. De regels in de Ambtenarenwet bepalen wat wel en niet toegestaan is. Een overheidswerkgever moet integriteitsbeleid opstellen om nadere invulling te geven aan die regels en in de organisatie afspraken maken over de toepassing ervan, bijvoorbeeld in de vorm van een Handboek Personeel.

De invoering van de Wnra, het vaststellen van de BIO als overheidsbrede baseline voor informatiebeveiliging per 1 januari 2020 en de reeds bestaande AVG vormen samen een aanleiding om de banden tussen de gemeentelijke HRM-medewerkers, de CISO en de PO te versterken.

Beleid

Op grond van artikel 4, eerste lid van de Ambtenarenwet 2017 is een integriteitsbeleid als vast onderdeel van het personeelsbeleid verplicht. Onderdeel daarvan is het bevorderen van integriteitsbewustzijn en het voorkomen van misbruik van bevoegdheden, bijvoorbeeld door maatregelen te treffen als screening van personeel en het toepassen van functiescheiding en functieroulatie in geval van kwetsbare functies.

De verplichting om een vastgesteld screeningsbeleid te hebben vinden we in het kader van veilig personeel ook terug in de Baseline Informatiebeveiliging Overheid (BIO). De BIO stelt dat op basis van een risicoafweging moet worden vastgesteld voor welke functie het overleggen van een VOG vereist is (BIO 7.1.1.1). Vanuit de Algemene Verordening Gegevensbescherming (AVG) bezien vallen een screeningsbeleid en functiescheiding onder beveiligingsmaatregelen (art. 32 AVG). Let wel dat screening ingrijpend kan zijn voor de betreffende medewerkers. Er zijn dan ook voorwaarden gesteld aan screeningen.[1]

Integriteit speelt zowel in het personeelsbeleid als in het informatiebeveiligingsbeleid en in de AVG een rol. Zorg dus voor samenhang tussen deze onderdelen in het opstellen en vaststellen van het integriteitsbeleid in uw gemeente.

Bewustzijn medewerkers

Het integriteitsbeleid wordt vast onderdeel van het personeelsbeleid door in ieder geval integriteit in functioneringsgesprekken en werkoverleg aan de orde te stellen en scholing en vorming op het gebied van integriteit aan te bieden. Deze verplichting is vastgelegd in artikel 4, tweede lid van de Ambtenarenwet 2017.

Scholing en vorming is ook voor de informatiebeveiliging en de gegevensbescherming van belang. In het kader van de BIO (7.2.2) behoren alle medewerkers van de organisatie een passende bewustwordingsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie. Zorgvuldige omgang met persoonsgegevens is verder uiteraard de kern van de AVG.

CISO en PO zijn vaak zelf al bezig is met bewustwordingscampagnes. Maar het betekent winst voor de organisatie als ook HRM erbij betrokken is. Integriteit vertaalt zich in veilig en bewust gedrag. Veilig gedrag begint bij de werving en selectie van personeel. Bewust gedrag vereist de juiste voorlichting over wat gedrag onveilig maakt. Laat in het introductieprogramma voor nieuwe medewerkers naast aandacht voor ARBO-afspraken vanuit HRM ook de CISO en PO aandacht besteden aan veilig werken in de organisatie. Zorg dat u alledrie een rol heeft in het introductieprogramma.

Voorkomen misbruik van bevoegdheden

Elke overheidswerkgever heeft een zorgplicht voor de werknemers. Dit betekent onder andere dat de werkgever zijn ambtenaren beschermt tegen integriteitsrisico's, door de organisatie en werkprocessen daarop in te richten, zoals het toepassen van functiescheiding (Aw, artikel 4, eerste lid). Om integriteitsrisico's te voorkomen, moet duidelijk zijn in welke functies die risico's zich voordoen. Dat maakt goede functiebeschrijvingen noodzakelijk. In de BIO is als verplichte maatregel in relatie met het beheer van toegangsrechten van de gebruikers de eis opgenomen dat op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven (9.2.2.2). Deze risicoafweging vindt plaats door de proceseigenaar. Betrek voor de juiste inschatting van risico's de CISO en PO bij het uitvoeren van de risicoafweging en laat HRM de maatregelen tegen integriteitsrisico's vastleggen in functiebeschrijvingen.

Gedragscode

Een gedragscode integriteit geeft ambtenaren een kader voor integer handelen. Artikel 4, derde lid van de Ambtenarenwet stelt een gedragscode verplicht. Een gedragscode geeft een overzicht van de belangrijkste afspraken op het gebied van integriteit. Het biedt een houvast bij het maken van afwegingen en het nemen van beslissingen, maar een gedragscode kan nooit in elke denkbare situatie voorzien. Ook kunnen de omstandigheden waarin ambtenaren werken wijzigen, denk bijvoorbeeld aan de

ontwikkelingen rondom sociale media. In de BIO wordt de eis gesteld dat gedragsregels voor het gebruik van bedrijfsmiddelen aantoonbaar bekend zijn gemaakt aan alle medewerkers (8.1.3.1). Onderdeel van de gedragscode zou in elk geval moeten zijn, dat alle medewerkers (intern en extern) bij hun aanstelling en functiewisseling gewezen worden op hun verantwoordelijkheden ten aanzien van informatiebeveiliging en privacy. Dat geldt ook na uitdiensttreding. De voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging moeten eenvoudig toegankelijk zijn (7.1.2.1). Een manier om aan deze eis uit de BIO te voldoen is openbaarmaking via intranet. Hetzelfde geldt uiteraard ook voor regelingen en instructies over privacy. Medewerkers dienen periodiek training te krijgen over deze regelingen en instructies. Het opstellen van de gedragscode vraagt om afstemming tussen HRM, CISO en PO. Door samen op te trekken wordt integer handelen verbonden aan gedragsregels die in het kader van omgang met bedrijfsmiddelen en persoonsgegevens moeten worden nageleefd.

Geheimhouding

Naast de verplichting tot het afleggen van de ambtseed of de belofte (Aw, artikel 7) is er voor de ambtenaar en de gewezen ambtenaar de verplichting tot geheimhouding van hetgeen hen in verband met hun functie ter kennis is gekomen, voor zover die verplichting uit de aard der zaak volgt (Aw, artikel 9). De bescherming van bedrijfsinformatie is ook in de BIO als verplichte maatregel vastgelegd (7.2.2.1).

Bedrijfsinformatie kan ook persoonsgegevens bevatten. In dat kader is een geheimhoudingsplicht ook relevant voor de AVG. Daarnaast zijn er andere vormen van geheimhouding, zoals de plicht om zich als goed werknemer en goed ambtenaar te gedragen en de geheimhoudingsplicht uit art. 272 Wetboek van Strafrecht. HRM, CISO en PO bepalen samen met de proceseigenaren voor welke functies een geheimhoudingsverklaring is vereist.

Jaarlijkse verantwoording over het integriteitsbeleid

Vanaf 2020 moeten overheidswerkgevers jaarlijks een verantwoording over het door hen gevoerde integriteitsbeleid openbaar maken. Dat staat in artikel 4, vierde lid van de Ambtenarenwet 2017.
De vorm waarin dit plaatsvindt is vrij. Dat kan in de vorm van een afzonderlijk integriteitsjaarverslag, maar dat hoeft niet. Het kan bijvoorbeeld ook een onderdeel zijn van een al bestaande jaarlijkse verantwoording.

Zoek voor de jaarlijkse verantwoording vanuit HRM aansluiting bij de jaarlijkse rapportage in de P&C-cyclus over informatiebeveiliging en privacy door CISO en PO, al dan niet gecombineerd met de jaarrapportage van de FG. Uiteindelijk is integriteit van medewerkers een belangrijke factor voor de betrouwbaarheid van de informatiebeveiliging en privacy.

Aan de slag

De raakvlakken die er ten aanzien van integriteit bestaan tussen HRM, CISO en PO maken het zeer gewenst dat deze partijen elkaar vinden binnen de organisatie. Misschien is het voor u een open deur en vindt u die samenwerking vanzelfsprekend. Feit is dat in veel gemeenten de genoemde raakvlakken concreet maken dat er meerwaarde te behalen is uit het vinden van elkaar. Houd elkaar up-to-date bij ontwikkelingen op het gebied van (integriteits-) bewustzijn. Betrek ook de afdeling of medewerker communicatie actief in het proces. Zorg dat de boodschap, de bewoording daarvan en de communicatiekanalen zodanig worden ingezet dat het integriteitsbeleid en de vereisten voor bewust veilig gedrag bekend raken en landen in de gehele organisatie.

Tot slot

In de handreiking ‘Personeelsbeleid gemeente’[2] en de handreiking ‘Screening personeel’[3] van de IBD zijn concrete aanbevelingen opgenomen om integriteit van medewerkers te borgen in beleid en procedures. In de handreiking “Verhogen bewustzijn informatiebeveiliging” is een structurele aanpak van het verhogen van het beveiligingsbewustzijn binnen de organisatie beschreven. Ook relevant is de handreiking ‘Geheimhoudingsverklaringen’.[4] Daarnaast is op de website van de VNG een toolkit beschikbaar met praktische informatie over de verschillende aspecten van integriteit voor ambtenaren.[5] De bijgaande tabel geeft de samenhang weer tussen de in de Ambtenarenwet 2017 vastgelegde wettelijke eisen, de verplichte maatregelen uit de BIO die in deze factsheet zijn benoemd en de relevante maatregelen uit het AVG Borgingsproduct.[6]

Eindnoten

1 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-uitkering/screening#welke-eisen-stelt-de-privacywetgeving-aan-screening-4613
2 https://www.informatiebeveiligingsdienst.nl/product/personeelsbeleid/
3 https://www.informatiebeveiligingsdienst.nl/product/handleiding-screening-personeel/
4 https://www.informatiebeveiligingsdienst.nl/product/geheimhoudingsverklaringen/
5 https://vng.nl/artikelen/introductie-toolkit-integriteit-voor-ambtenaren
6 https://www.informatiebeveiligingsdienst.nl/product/criteria-borging-avg-borgingsproduct-gegevensbescherming-in-de-gemeentelijke-organisatie/

Meer informatie

Meer informatie over onze dienstverlening vindt u in de andere factsheets van de IBD en op de website www.informatiebeveiligingsdienst.nl. De helpdesk van de IBD is te bereiken tijdens kantooruren van 9:00 tot 17:00 uur op het nummer 070 204 55 11 of via het e-mailadres info@IBDgemeenten.nl. De CERT van de IBD is 24x7 bereikbaar via 070 204 55 11 (instructies voor het piketnummer op de voicemail).

Ambtenarenwet 2017		Baseline Informatiebeveiliging Overheid (BIO)		AVG Borgingsproduct	
3a	Overheidswerkgevers kunnen een onderzoek naar de geschiktheid en de bekwaamheid voor een functie als ambtenaar doen.	7.1.1.1	Elke organisatie heeft een vastgesteld screeningsbeleid. Bij indiensttreding en bij functiewijziging kan een Verklaring Omtrent het Gedrag (VOG) gevraagd worden.		
4.1	Een overheidswerkgever voert een integriteitsbeleid dat is gericht op het bevorderen van goed ambtelijk handelen en dat in ieder geval aandacht besteedt aan het bevorderen van integriteitsbewustzijn en aan het voorkomen van misbruik van bevoegdheden, belangenverstrengeling en discriminatie.	7.2.2	Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	12.2 12.3	Medewerkers worden actief getraind om de kennis van het privacyrecht en het privacybewustzijn op het specifieke domein te verhogen. Medewerkers worden doorlopend bewust gemaakt van de risico's en randvoorwaarden bij de omgang met persoonsgegevens, bijvoorbeeld door interne opleidingen of trainingen, het delen van DPIA's en het verstrekken van adviesmateriaal
4.2	Een overheidswerkgever zorgt ervoor dat het integriteitsbeleid een vast onderdeel uitmaakt van het personeelsbeleid, in ieder geval door integriteit in functioneringsgesprekken en werkoverleg aan de orde te stellen en door het aanbieden van scholing en vorming op het gebied van integriteit.	7.2.2.2	Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd.		
4.3	Een overheidswerkgever draagt zorg voor de totstandkoming van een gedragscode voor goed ambtelijk handelen.	6.2.1.2a 7.1.2.1 8.1.3.1	In bewustwordingsprogramma's komen gedragsaspecten van veilig mobiel werken aan de orde. Alle medewerkers (intern en extern) zijn bij hun aanstelling of functiewisseling gewezen op hun verantwoordelijkheden ten aanzien van informatiebeveiliging. De voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging zijn eenvoudig toegankelijk. Alle medewerkers zijn aantoonbaar gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen.	12.1	Op afdelingsniveau zijn – wanneer noodzakelijk - actuele protocollen en procedures beschikbaar over de wijze van omgang met persoonsgegevens.

Ambtenarenwet 2017		Baseline Informatiebeveiliging Overheid (BIO)		AVG Borgingsproduct	
4.4	Een overheidswerkgever maakt jaarlijks een verantwoording met betrekking tot de uitvoering van dit artikel openbaar.	18.2.2.1	In de P&C-cyclus wordt gerapporteerd over informatiebeveiliging, resulterend in een jaarlijks af te geven In Control Verklaring (ICV) over de informatiebeveiliging. Indien voldoende herkenbaar kan de ICV voor informatiebeveiliging onderdeel zijn van de reguliere, generieke verantwoording.	4.1 4.2 7.1	Periodiek worden controles uitgevoerd om de juiste werking van de getroffen beveiligingsmaatregelen te controleren. Rapportages worden beschikbaar gesteld aan de verantwoordelijke. De FG doet periodiek verslag aan het verantwoordelijk bestuursorgaan over de omgang met persoonsgegevens binnen de gemeente.
7 9	De ambtenaar legt een eed of belofte af, overeenkomstig een bij algemene maatregel van bestuur vastgesteld formulier, dat voor verschillende functies verschillend kan zijn. De ambtenaar en de gewezen ambtenaar zijn verplicht tot geheimhouding van hetgeen hen in verband met hun functie ter kennis is gekomen, voor zover die verplichting uit de aard der zaak volgt.	7.2.2.1	Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen.	13.1 13.2 13.3	Alle ambtenaren zijn op de hoogte van de algemene geheimhoudingsplicht voor ambtenaren. Medewerkers die te maken hebben met bijzondere persoonsgegevens hebben tevens een specifieke geheimhoudingsverklaring ondertekend die ziet op het verwerken van die bijzondere persoonsgegevens. Alle externen hebben een integriteits- en geheimhoudingsverklaring ondertekend.