

shares

Maart 2025

Digitale veiligheid

- ✓ Poging tot CEO-fraude
- ✓ Facts & Figures
- ✓ Informatieveiligheid
- ✓ Werk & Uitdaging

 Ga naar de voorpagina

 Vorige pagina

 Volgende pagina

Inhoud



Pagina 4 en 5

Voorwoord
Cees Boele over
preventie en voorlichting



Pagina 6 t/m 11

Poging tot CEO-fraude
Wake-up call bij
gemeente Papendrecht



Pagina 12 en 13

Fact & Figures
Blijf Altijd Alert
met Sir Askalot



Pagina 14

Tips & Tricks
Scheur 'm uit en hang het
op bij je werkplek



Pagina 15 t/m 19

Informatieveiligheid
Hoe houden we data veilig
in de Drechtsteden?



Pagina 20 en 21

Werk & Uitdaging
Functionaris Gegevens-
bescherming aan het woord

**“Digitale veiligheid
is een gedeelde
verantwoordelijkheid.
Geen keuze, maar
een noodzaak.”**

Voorwoord

Cees Boele

Directeur Bedrijfsvoering Drechtsteden

Digitale veiligheid. Niet langer een keuze maar een noodzaak. In een wereld waarin technologie zich razendsnel ontwikkelt en digitale aanvallen steeds geavanceerder worden, is het van essentieel belang dat we ons wapenen tegen deze gevaren. Daarom hebben we deze gehele editie Shares aan dit onderwerp gewijd met een sterke focus op preventie en voorlichting.

We zagen het vorig jaar in Papendrecht. Een e-mail van de “gemeentesecretaris” met een dringend, ietwat buitengewoon verzoek, zorgde voor argwaan bij de ontvangende collega. Doorklikken of gehoor geven aan een dergelijk verzoek kan catastrofale gevolgen hebben. Door bewustwording (‘klopt deze e-mail en is het e-mailadres van de afzender juist?’), navragen (via een ander kanaal contact opnemen met de afzender) en het nemen van voorzorgsmaatregelen is dit incident gelukkig goed afgelopen. Maar het had ook anders kunnen aflopen en iedereen kan dit overkomen.

Wat ik maar wil zeggen is, digitale veiligheid is een gedeelde verantwoordelijkheid. In dit magazine laten we verschillende collega’s aan het woord en hebben we belangrijke tips voor je op een rijtje gezet. Lees het rustig door, vergroot je kennis en bewustwording, maar blijf vooral alert! ■

**“Dit was een
wake-up call
voor ons
allemaal.”**



Joost Ansems

Gemeentesecretaris gemeente Papendrecht



Marco Penders

Teamleider juridische zaken,
informatiemanagement en financiën
gemeente Papendrecht

Poging tot CEO-fraude bij gemeente Papendrecht

Marco Penders is teamleider juridische zaken, informatiemanagement en financiën bij gemeente Papendrecht. Dat hij over mensenkennis beschikt, bewees Marco afgelopen april maar weer eens. Er zat een e-mail van gemeentesecretaris Joost Ansems in zijn inbox. Maar de toon en het woordgebruik in het bericht waren niet 'des Joost'. Het bleek te gaan om een poging tot CEO-fraude: een vals verzoek om gegevens of geld dat van de bedrijfsmanager lijkt te komen. ▶

“Wat is er aan de hand?”

Marco: “In de aanhef van de betreffende e-mail stond alleen ‘Joost’. Toen dacht ik: ‘Oké, dit klinkt niet goed. Wat is er aan de hand?’”. Ik wilde reageren, maar iets hield me tegen. Dus ik heb Joost geappt en hij belde meteen terug.” Joost: “Ik had op dat moment al meerdere signalen gekregen van collega’s die dezelfde e-mail hadden gekregen. Zo is het balletje gaan rollen.”

Een gestolen identiteit

Marco: “Ik heb gelijk de informatiebeveiligingsadviseur op de hoogte gebracht. Die plaatste direct een berichtje op ons intranet en maakte melding bij Hans Baaten – de Chief Information Security Officer (CISO) van Bedrijfsvoering Drechtsteden.” Joost: “Eén medewerker had op de e-mail gereageerd. Met hem is ook nog WhatsApp-contact geweest – compleet met mijn naam en foto. Dat vind ik nog steeds een beangstigende gedachte.”

Snel handelen

Marco: “De afzender vroeg om e-mailadressen en andere persoonsgegevens van collega’s. Het was echt bedoeld om toegang te krijgen tot personeelsleden en hun wachtwoorden. Door het snelle handelen is dat niet gebeurd. Het e-mailadres van de afzender – een hotmailadres – is meteen geblokkeerd. En Bedrijfsvoering Drechtsteden heeft de trackrecords gecontroleerd. Daaruit bleek dat er geen gegevens buiten de organisatie zijn terechtgekomen.”

Investeren in awareness

Joost: “De gevolgen vielen nu mee. Maar het confronterende is: je voorkomt dit soort dingen nooit helemaal. Dus wat betreft digitale veiligheid moeten we vooral investeren in bewustwording. Marco: “Mensen zijn bijvoorbeeld gauw geneigd te reageren op een e-mail. Dat doe ik zelf ook. Er zijn echter altijd signalen als iets niet klopt. Past het bericht binnen het werk wat ▶

Wat is CEO-fraude?

CEO-fraude is een vorm van social engineering waarbij criminelen zich voordoen als bestuurder, secretaris, directeur of manager van een organisatie om financiële of gevoelige informatie te stelen. Ze sturen geloofwaardige e-mails, app-berichten of telefoontjes en dringen aan op het doen van betalingen of het verstrekken van gegevens. Je kunt CEO-fraude herkennen door te letten op ongebruikelijke taal, onverwachte urgentie en afwijkende e-mailadressen. Als je vermoedt dat een verzoek van een bestuurder, directeur of manager niet in de haak is, neem dan contact op met de medewerker/afzender via de contactgegevens uit Outlook (niet uit het ontvangen bericht!). Zo bescherm je je organisatie tegen deze bedreiging.

“Het is niet de vraag óf er weer cyberfraude plaatsvindt, maar wanneer.”



je doet? Is het normaal dat iemand bij jou op de lijn komt?”

Kennis, expertise en professionele slagkracht

Marco: “Dit hele voorval heeft ertoe geleid dat informatiebeveiliging bij gemeente Papendrecht in een stroomversnelling is terechtgekomen. We zijn nu bezig met business continue management – om de processen en cruciale informatiestromen voor de gemeentelijke uitvoering in kaart te brengen. Joost: “Dat doen we samen met Bedrijfsvoering Drechtsteden. Want zelf krijgen we alles nooit helemaal ingeregeld en georganiseerd. Als je ziet hoe geraffineerd hackers te werk gaan,

dan heb je daar extra kennis, expertise en professionele slagkracht voor nodig.”

Wisselwerking

Marco: “We zijn blij met de hulp van Bedrijfsvoering Drechtsteden. Maar op sommige vlakken nemen we het heft meer in eigen handen, zoals met het business continue management. De rest van de regio maakt dankbaar gebruik van onze stappen. Zo helpen we elkaar op weg. Wat mij betreft snijdt het mes dan ook aan twee kanten: Bedrijfsvoering Drechtsteden heeft iets te doen, maar ook lokaal hebben we wat te organiseren en regelen met elkaar. Beiden zijn verantwoordelijk.”

“Het grootste risico schuilt in menselijk handelen.”



Continu proces

Joost: “Vorig jaar hebben we nog meer kunnen investeren in informatiebeveiliging. In de perspectiefnota 2024 hebben we extra middelen gekregen om een extra informatiebeveiligingsadviseur in dienst te nemen. Het is namelijk niet meer de vraag óf er iets gebeurt, maar meer wannéér. Dan moet je klaar zijn om maatregelen te treffen en correcties te doen. We zijn ook heel scherp op de NIS2-voorbereidingen.” Marco: “Informatiebeveiliging blijft een continu proces. De wet- en regelgeving wordt steeds uitgebreider en de beveiligingstechnieken beter. Maar aan de andere kant: cybercriminelen bedenken ook steeds weer nieuwe dingen. En daar komt bij: welke maatregelen we ook treffen, 100% garantie hebben we nooit.”

Menselijk handelen

Joost: “Het grootste risico schuilt in menselijk handelen. In dit geval van CEO-fraude ging het goed. Dat vind ik ook zeker een compliment waard richting de organisatie, dat veel medewerkers zo alert waren.” Marco: “Maar ook hier valt zeker nog winst te behalen. Laatst was er een regionale phishingactie vanuit Bedrijfsvoering Drechtsteden, waarbij 40% van onze werknemers op een ‘valse link’ hebben geklikt. 20% van hen heeft dit gemeld. Het is des te belangrijk dat die bewustwordingscampagnes er zijn. Om nog meer besef te creëren, oplettend te zijn, maar ook om melding te maken als er iets fout is gegaan.” ■

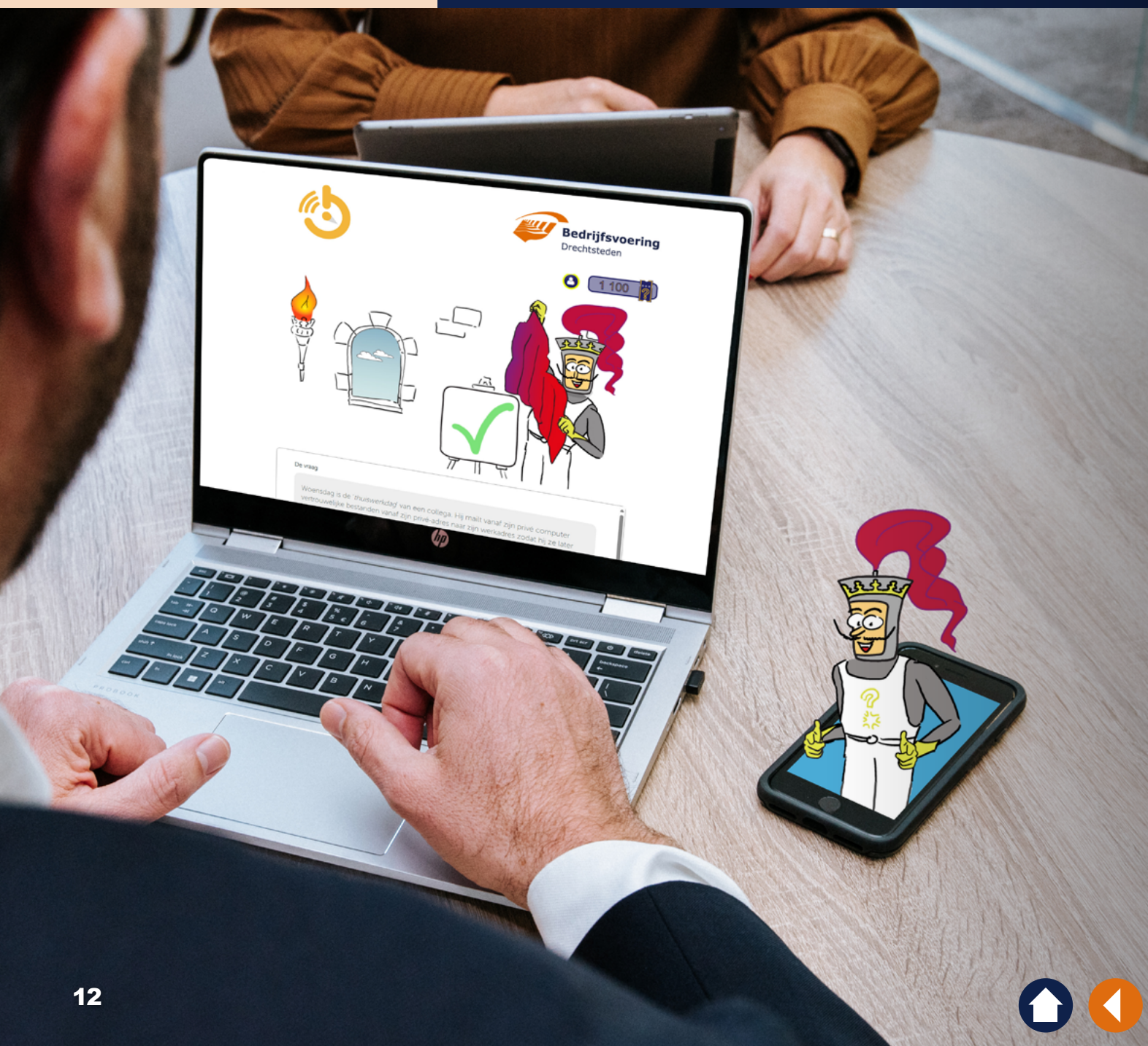
Facts & Figures

353.130

e-mails verstuurd
vanuit Sir Askalot sinds
1 november 2023

Top 3 Respondenten:

1. OZHZ
2. Papendrecht
3. Hendrik-Ido-Ambacht



Altijd Alert stuurt onder andere op:

- Voorzichtig omgaan met verdachte sites, e-mails, berichten, etc.
- Zakelijke informatie weghouden van onbevoegden.
- Alert zijn op risico's van clouddiensten, onbeveiligde internetverbindingen etc.

De Altijd Alert-groep binnen ons intranet is hét kennisplatform binnen Drechtsteden waar je trainingen en workshops kunt volgen op het gebied van informatieveiligheid. Hier kun je als medewerker je kennis ophalen, bewuster worden van digitale gevaren én van mogelijkheden om veiliger te werken.

Sir Askalot is het gezicht van dit platform en zal regelmatig op digitale deuren kloppen voor een paar prikkelende vragen. Weet jij hoe je moet handelen bij een beveiligingsincident?

Tips & tricks



Hoe herken je een verdachte e-mail?

- ✓ Onjuist afzendadres: let goed op de spelling van het mailadres!
- ✓ Spelfouten in het bericht, of onvolledige/onjuiste handtekening.
- ✓ Algemene begroeting in plaats van jouw naam (beste medewerker).
- ✓ Vragen persoonlijke gegevens in te vullen.
- ✓ Aanzetten tot spoed of urgentie benadrukken.



Niet openen! Het openen van de e-mail kan een spammer erop attenderen dat jouw mailadres in gebruik is of een onbeschermd apparaat in gevaar brengen.

Verdachte e-mail? Meld het op SID via 'Direct naar' > Beveiligingsincident of datalek. Kies vervolgens voor Spam en/of Phishing.



Op een verkeerde link geklikt? Maak z.s.m. een melding via SID, zodat onze medewerkers schade kunnen beperken of voorkomen.

Beantwoord de e-mail niet, tenzij je zeker weet dat deze afkomstig is van een betrouwbare afzender.



Klik niet op linkjes, ook niet op de 'unsubscribe' knop. Download geén bijlagen uit de e-mail.

Verwijder ná het melden de e-mail uit je inbox, zodat je deze in de toekomst niet per ongeluk opent of hier iets in aanklikt.



Voer je Windows updates altijd z.s.m. uit, zo ben je goed beschermd volgens de laatste beveiligingsstandaarden.

Voer geén persoonlijke of financiële informatie in op pop-up schermen.



“Hoe houden we data veilig?”

Hans Baaten

Chief Information Security Officer (CISO), Bedrijfsvoering Drechtsteden

“Informatieveiligheid lijkt misschien een abstract begrip, maar voor mij gaat het om iets heel concreets: het beschermen van mensen. Want als hun persoonlijke gegevens op straat liggen, kan dat grote gevolgen hebben. Financiële schade, reputatieverlies, of zelfs identiteitsfraude. Die risico's mogen we niet negeren.” Met deze woorden vat Hans Baaten, de Chief Information Security Officer (CISO) van Drechtsteden, de essentie van zijn werk samen. Informatieveiligheid is een gezamenlijke verantwoordelijkheid van iedereen binnen de Drechtsteden, waarin medewerkers én technische experts een onmisbare rol spelen. “Samen vormen we de verdedigingslijnes.” ▶



Informatieveiligheid voor 300.000 burgers en 5.000 medewerkers. Waarom is dat zo belangrijk?

Bedrijfsvoering Drechtsteden werkt met 10 partnerorganisaties. 5.000 collega's verwerken dagelijks allerlei vertrouwelijke informatie. "We hebben het over persoonsgegevens, zoals adressen, gezondheidsdossiers en financiële details van 300.000 inwoners, maar ook over strategische plannen van de Drechtstedelijke organisaties," legt Hans uit. "Als die in verkeerde handen vallen, heeft dat een enorme - negatieve - impact. Niet alleen voor individuen, voor onze hele maatschappij."

Dagelijkse digitale aanvallen

Die dreiging komt van alle kanten. "Soms gaat het om een simpele

menselijke fout, zoals een brief sturen naar de verkeerde persoon. Steeds vaker komt het gevaar van buitenaf: cybercriminelen, phishingmails, of grootschalige aanvallen zoals DDoS - waarbij een aanvaller duizenden opdrachten geeft aan bijvoorbeeld www.dordrecht.nl, en daarmee alles kan platleggen. En vergeet de wereldwijde spanningen tussen landen niet. Digitale aanvallen horen vandaag de dag bij een moderne manier van oorlogsvoering.

Onze aanpak: vier verdedigingslijnes

Hoe zorgen we ervoor dat de overheidsorganisaties in de Drechtsteden digitaal weerbaar zijn? We werken gezamenlijk met het bewezen model om

informatieveiligheid te organiseren: het 'Lines of Defense'-model. Hans licht het toe:

1. De eerste linie: de werkvloer

"De werkvloer is waar het gebeurt. Medewerkers en lijnmanagers weten welke informatie ze verwerken en welke risico's daaraan verbonden zijn. Hier begint de beveiliging: met een sterk wachtwoord, oplettendheid bij verdachte e-mails en het melden van afwijkingen."

2. De tweede linie: specialisten en ondersteuning

"Mijn team van veiligheidsadviseurs en ik staan klaar om de eerste linie te ondersteunen. Op strategisch, tactisch én operationeel niveau. We

maken beleid, leren hoe je risico's herkent en adviseren over extra beveiligingsmaatregelen. Denk aan het blokkeren van verdachte websites, het aanpakken van kwetsbaarheden in applicaties en het beveiligen van onze telefoons en laptops. KPN is daarin onze technische partner. Maar juist omdat onze medewerkers in de eerste lijn erg belangrijk zijn bij het voorkomen van security-incidenten, organiseren we (verplichte) trainingen en workshops."

3. De derde linie: toezicht en controle

"In de derde linie houden we elkaar scherp. Doen we wat we in het beleid hebben afgesproken? En waar kan het beter? Beheerders, controllers en auditors controleren dit periodiek." ▶

Zo kan het misgaan: Stad Antwerpen gehackt

In 2023 werd stad Antwerpen slachtoffer van een ransomware-aanval. Via een 'achterdeur' in verouderde software kwamen hackers binnen, die alle systemen en gegevens versleutelden. Maandenlang was digitale dienstverlening onmogelijk. De schade: 78 miljoen euro. Zo zie je maar, informatieveiligheid is essentieel.

Hans voegt toe: "In aanvulling op dit model, hebben we in de Drechtsteden nog een vierde linie: de onafhankelijke, externe auditor. Hiermee legt het college van burgemeester en wethouders verantwoording af aan hun toezichthouders: ministeries en de gemeenteraad - en daarmee ook aan onze inwoners. Zo is de cirkel netjes rond."

Nog weerbaarder met NIS2: de nieuwe standaard voor veiligheid

In 2024 is de Europese NIS2-richtlijn van kracht geworden: Network and Information Security directive. In Nederland kennen we deze in 2025 als de Cyberbeveiligingswet (Cbw). Het doel? De digitale weerbaarheid van de maatschappij verhogen, zodat we samen beter bestand zijn tegen cyberaanvallen. "NIS2 maakt duidelijk welke belangrijke rol de besturen en directies hebben. En het legt de lat hoger: je moet op elk

moment kunnen aantonen (aan de externe toezichthouder) dat je jouw cyberrisico's kent en daar passende maatregelen bij neemt," vertelt Hans. "Het helpt ons om de keten van inwoners, organisaties, en allerlei leveranciers goed te beveiligen."

Wat kun je zelf doen?

Volgens Hans is informatieveiligheid een mooi samenspel van organisatie, techniek, fysieke beveiliging én een forse dosis gezond veiligheidsbewustzijn. "We worden dagelijks bestookt met aanvallen. Een hacker heeft maar één kwetsbaar punt nodig om binnen te komen. Daarom moet iedereen alert blijven. Of je nu beleidsmaker, manager, servicemedewerker of applicatiebeheerder bent: neem informatieveiligheid serieus."

Meer weten?

Neem gerust contact op met Hans via hans.baaten@drechtsteden.nl. Hij helpt je graag verder. ■



Tips van Hans

- Gebruik altijd tweefactorauthenticatie (2FA): inloggen in twee stappen.
- Klik niet op verdachte links in e-mails of berichten.
- Meld verdachte situaties direct bij het serviceloket: 078 - 770 8008.

"We zijn zuinig op de gegevens van onze inwoners."



Het uitwisselen van gegevens tussen je zakelijke en privé omgeving op je laptop of smartphone brengt aanzienlijke risico's met zich mee. Voor je het weet breng je vertrouwelijke bedrijfs- of persoonsgegevens naar buiten en veroorzaak je een datalek. Maar ook door linkjes, documenten en afbeeldingen van buiten je zakelijke bubbel naar binnen te kopiëren, loop je een behoorlijk risico op het binnenhalen van kwaadaardige software (malware).

Slimme technische beveiligingsmaatregelen werken als goede remmen op je auto; je kunt stevig veilig doorrijden. Dat is onze basisbeveiliging. Maar als je je onverantwoord gedraagt, dan vlieg je alsnog uit de bocht.

Werk & Uitdaging

Zorgvuldig omgaan met persoonsgegevens? Dat zijn we verplicht aan onze inwoners.

"Privacy draait niet om het volgen van regels. Het gaat vooral om het vertrouwen van inwoners en medewerkers - dat er zorgvuldig met hun gegevens wordt omgegaan. Of dat zo is, hangt af van onze keuzes: Waarom hang je camera's op? Wat doe je met social media? Gebruik je WhatsApp ook zakelijk? Privacy-bewustzijn is daarbij onmisbaar. Maar dat gaat vaak pas een rol spelen als het om eigen gegevens gaat.

Slordig omgaan met persoonsgegevens - van wie dan ook - kan veel schade aanrichten. Daarom is het zo belangrijk dat je het goed doet. En dat je je bewust bent van de gevolgen van het delen van persoonsgegevens.

Neem WhatsApp. Dat gebruiken we allemaal. Maar dit is echt bedoeld voor zaken als 'Neem jij het brood mee', 'We zitten in kamer zes' en 'Ik pik Jan wel op'. Niet voor notulen, documenten en inloggegevens. Als je (veilig) wilt samenwerken, zijn er andere kanalen, zoals

vakapplicaties of Teams. En weet je niet precies wat voor jou de handigste communicatiewijze is? Of heb je andere vragen? Ga advies halen bij de Informatiebeveiligingsdeskundigen en de Informatiemanagers. Of loop naar de privacy coördinator en zeg: 'Ik kom hier gewoon niet uit'. Want geen vraag is te gek.

Naast toezichthouder op de naleving van de Algemene Verordening Gegevensbescherming (AVG), ben ik als Functionaris Gegevensbescherming ook adviseur en coach. Binnen elk project let ik erop of persoonsgegevens zorgvuldig worden verwerkt en denk hierin mee. Daarbij kijk ik altijd naar het belang van alle betrokkenen. Want het vertrouwen van je inwoners? Daar ben je als organisatie verantwoordelijk voor.

Ik zou het mooi vinden als steeds meer mensen denken: 'We staan samen in dienst van onze inwoners, ook bij het gebruik van persoonsgegevens'. Dat lukt alleen als steeds meer medewerkers weten waar ze terecht kunnen met vragen en het belang van privacy en informatiebeveiliging inzien. Daaraan wil ik graag bijdragen." ■

Wil je meer weten over de Algemene Verordening Gegevensbescherming?
Of over het werk van de Functionaris Gegevensbescherming?
Stuur een mail naar FG@rechtsteden.nl!

Colette Kersten

Sinds juni 2023 Functionaris Gegevensbescherming bij de zeven Drechtstedengemeenten en de Omgevingsdienst.





“Informatieveiligheid heeft belang bij een forse dosis gezond veiligheidsbewustzijn van ons allemaal.”

Colofon

Tekst - Fay Huigen en
Sandra Borger

Eindredactie - Peter Manders en
Team Communicatie Regio

Fotografie - Daniëlle Vliegenthart
en Maartje Brockbernd

Vormgeving - Elle Smeets

Postadres

Postbus 8
3300 AP Dordrecht

Telefoonnummer

078 - 770 8000

