HUIS VOOR KLOKKENLUIDERS

PUBLICATIE KENNIS & PREVENTIE

Een integere digitale werkomgeving

20 april 2026

Een integere digitale werkomgeving

Fout! De hyperlinkverwijzing is ongeldig.

SAMENVATTING

Deze brochure[1] is gemaakt voor werkgevers die hun integriteitsbeleid willen actualiseren. En dan specifiek op het gebied van integriteitsrisico's die (het gebruik van) digitale middelen met zich mee kunnen brengen. De brochure gaat vooral over de implicaties van middelen die gebruik maken van *generative/agentic* AI[2] in het bijzonder.

De brochure schetst een beeld van hoe een integere digitale werkomgeving eruit kan zien en biedt handvaten voor organisaties hoe om te gaan met de specifieke integriteitsrisico's. De brochure gebruikt de integriteitsinfrastructuur van het Huis voor Klokkenluiders om tips, aandachtspunten en vragen mee te geven ten behoeve van een integere digitale werkomgeving.

De belangrijkste tips zijn samengevat:[3]

1. Zorg voor **duidelijke kaders** en **visie** op integer digitaal werken: communiceer helder welke regels en verwachtingen gelden voor het gebruik van digitale middelen, leg de visie over digitale integriteit van de directie vast in het integriteitsbeleid en neem een beschrijving van integer digitaal gedrag op in de gedragscode van uw organisatie.
2. Richt **risicobeheersing** en **compliance** in: voer een risicoanalyse uit voor het gebruik van digitale middelen met aandacht voor functie-specifieke risico's en de impact van AI. Zorg voor transparantie en verantwoording over de inzet van digitale middelen en houdt rekening met wet- en regelgeving zoals de AI Act om boetes en reputatieschade te voorkomen.
3. Beperk AI-gebruik in HR-processen en zorg bij gebruik voor **menselijke toetsing** en **afweging**. Toets beslissingen die AI maakt en voorkom overmatige monitoring van medewerkers.
4. Investeer in **kennis** en **deskundigheid** door training aan te bieden in AI geletterdheid. Zorg voor een **open meldcultuur** door signalen serieus te nemen.
5. **Evalueer** en streef naar **continue verbetering** door een plan-do-check-act cyclus toe te passen, openlijk te communiceren over fouten en leerpunten en regelmatig digitale middelen te evalueren op betrouwbaarheid, uitlegbaarheid en doelgerichtheid.

Hoe kan uw organisatie deze vijf punten concreet inzetten om een cultuur van integere digitale werkomgeving te versterken? In de hoofdstukken die volgen, worden de bovenstaande punten voorzien van concrete handvatten.

---

[1] Deze brochure is gebaseerd op het eerdere werk van Kristien Verbraeke bij het Huis voor Klokkenluiders. Op deze versie van de brochure las vanuit het Ministerie van Binnenlandse Zaken AI-expert Jurriaan Raaijmakers mee. Het Huis is hem dankbaar voor zijn bijdrage.

[2] Met *generatieve AI* bedoelt het Huis voor Klokkenluiders een algoritme dat reageert op een prompt door content te creëren, zoals een tekst of een afbeelding. Met *agentic AI* bedoelt wij een systeem dat proactief en autonoom complexe taken uitvoert die bestaan uit meerdere stappen.

[3] Bij wijze van experiment is deze samenvatting gemaakt met behulp van Le Chat AI.

Inhoud

1. INTRODUCTIE

Ontwikkelingen in het digitale domein gaan snel. Deze ontwikkelingen bieden kansen. Om deze kansen op een verantwoorde manier te benutten, moeten organisaties hun integriteitsbeleid hierop aanpassen. Digitale middelen, met name artificiële intelligentie (AI), brengen specifieke integriteitsrisico's met zich mee en vereisen aandacht voor integer gebruik in alle onderdelen van de organisatie. Dit is extra belangrijk, omdat regelgeving op dit terrein vaak achterloopt op de snelle ontwikkelingen. Naast aandacht hebben voor integriteitsrisico's en voldoen aan de wettelijke vereisten, is het van belang om regelmatig het gesprek te voeren over de morele afwegingen bij de inzet van digitale middelen.

Digitale middelen worden gebruikt in verschillende werkprocessen binnen een organisatie. Hierbij kan gedacht worden aan:

- Communicatie en samenwerking
- Documentbeheer en -opslag en online samenwerkingsomgevingen
- Project- en taakmanagement
- Bedrijfssoftware als CRM-systemen en ERP-systemen
- Data-analyse en -rapportage
- AI-toepassingen voor het automatiseren werkprocessen, het genereren van inzichten en voorsorteren op besluitvorming

De snelle veranderingen in het digitale domein kunnen mogelijk ongewenste (neven)effecten met zich mee brengen. De technologie is namelijk soms zo ingewikkeld dat het niet altijd duidelijk of bekend is hoe ze precies werkt en hoe we bijvoorbeeld fouten kunnen herkennen en rechtzetten. Verder is het niet altijd duidelijk wat de bronnen zijn waar digitale middelen gebruik van maken, of waar informatie die wordt ingevoerd, eigenlijk terechtkomt en wie daar toegang toe heeft. Denk aan AI-toepassingen die informatie van het web gebruiken om een tekst te schrijven. Hoe betrouwbaar is die informatie en hoe zit het met auteursrechten? Wordt bedrijfsinformatie in de Cloud ongemerkt gebruikt om AI te trainen?

Wat is een integriteitsschending?
Het niet handelen overeenkomstig de daarvoor geldende morele waarden en normen en de daarmee samenhangende (spel)regels in een organisatie noemen we een integriteitsschending. De integriteitsschending noemen we een misstand als het maatschappelijk belang in het geding is. Dat is in geding als de schending een of meerdere individuele belangen overstijgt en als er ook sprake is van een patroon of structureel karakter of als de handeling of nalatigheid ernstig en omvangrijk is. Elke misstand is een integriteitsschending. Andersom is dat niet altijd zo. Integriteitsschendingen of misstanden in het gebruik van digitale middelen verdienen beiden aandacht. Waar we in deze brochure spreken over integriteitsschending, bedoelen we integriteitsschending of misstand.
Bij een integriteitsschending in het digitale domein kunt u denken aan het niet adequaat beschermen van persoonsgegevens, uw beslissingen baseren op onjuiste door AI-gegenereerde resultaten of het ongeautoriseerd toegang hebben tot gevoelige documenten.

WAT BETEKENT HET OM EEN INTEGERE DIGITALE OMGEVING TE HEBBEN?

Als een organisatie digitale systemen gebruikt, is het belangrijk dat hierbij aandacht is voor **wet- en regelgeving** rondom integriteit en digitalisering. Maar, wet- en regelgeving is nog in ontwikkeling. Ook als een organisatie zich aan alle wetten en regels houdt, kan deze schade veroorzaken. Daarom is het van belang om extra aandacht te hebben voor de **ethische aspecten** van de omgang met digitale middelen. Dit betekent dat er gekeken wordt naar de verschillende waarden die relevant zijn voor directie, medewerkers en andere belanghebbenden. Kort samengevat betekent een integere digitale werkomgeving:

1. **Beperkte afhankelijkheid** van digitale middelen en **menselijke controle** van digitale systemen.
2. Oog voor negatieve (bij)effecten van gebruik van digitale systemen, waarbij een **waarden- en belangenafweging** wordt gemaakt en **rechten** worden gerespecteerd.
3. Aandacht voor **juridische** en **maatschappelijke risico's** die zijn verbonden aan het gebruik van digitale middelen.
4. Ontwikkelen en **actualiseren van integriteitsbeleid** gericht op het digitale domein, inclusief periodieke risicoanalyses.

Juridisch kader
Zoals eerder benoemd, loopt de wet- en regelgeving op gebied van het reguleren van digitale innovatie (met name AI) achter op de snelle ontwikkelingen. Desalniettemin is het belangrijk om op de hoogte te zijn van de regelgeving die er al wel is op dit domein. Zo zijn er op Europees niveau de Digital Markets Act en de AI Act (zie voor meer informatie ook het Europees AI Bureau) en op nationaal niveau is de AVG een belangrijke wet. In het volgende hoofdstuk vind u wat hulpmiddelen die inzicht geven in voldoen aan deze wet- en regelgeving.
Voor de publieke sector en de overheid specifiek gelden meer regels. Denk daarbij aan de Wet Digitale Overheid, de Wet modernisering elektronisch bestuurlijk verkeer, de Cyberbeveiligingswet en de BIO-2-kaders. In de Overheidsbrede visie op Generatieve AI kunt u meer vinden over specifieke regels voor overheidsorganisaties op het gebied van AI. Voor publieke organisaties is er ook het Algoritmekader als kennisbank over geldende wet- en regelgeving.

2. HULPMIDDELEN

Er is al veel geschreven over ethische en juridische aspecten van digitalisering. Deze inzichten kunt u middels de onderstaande tools toepassen in uw organisatie, om toe te werken naar een integere digitale werkomgeving. Het Huis voor Klokkenluiders heeft een overzicht gemaakt van bruikbare hulpmiddelen die de zoektocht is tegengekomen. Bij ieder hulpmiddel staat wie het ontwikkeld heeft, en waar u het voor kan gebruiken. Omdat de techniek zo snel gaat, zijn er mogelijk al weer nieuwere (betere) hulpmiddelen te vinden.

2.1 WAARDEN- EN BELANGENAFWEGING

Voor het faciliteren van het gesprek over integer gebruik van digitale middelen kunt u verschillende gesprekstools gebruiken. De Utrecht Data School (DEDA) helpt organisaties met brainstormen over ethische overwegingen bij **datamanagement**. Het is een handige tool om inzicht te krijgen in de waarden die relevant zijn in de digitale werkomgeving, zoals privacy en betrouwbaarheid. Dit kan helpen bij het maken van een rechten- en belangenafweging bij de inzet van digitale middelen.
De AIIA (Rijksoverheid) is een tool die helpt met het afwegen van het doel en de noodzaak van de inzet van een digitaal middel ten opzichte van de impact op duurzaamheid en andere publieke waarden bij de inzet van **artificiële intelligentie** (AI). De tool kan gebruikt worden in alle fases van het werken met AI, van de inkoop van het digitale systeem tot het evalueren van de impact van AI in werkprocessen. Bij impact assessment van AI kan een organisatie ook de IAMA (Rijksoverheid) gebruiken: deze tool toetst de impact van AI op **mensenrechten**.

Meer dan alleen voldoen aan wet- en regelgeving
Het Huis voor Klokkenluiders heeft hulpmiddelen die betrekking hebben op moreel leren in het gebruik van digitale middelen opgenomen, omdat een integere digitale werkomgeving verder gaat dan handelen in lijn met de wet. Iets kan legaal zijn en tegelijkertijd maatschappelijk onwenselijk. Digitale middelen die draaien op AI zijn voor de efficiëntie van werkprocessen heel aantrekkelijk. Juist deze middelen die zakelijk aantrekkelijk zijn, verdienen extra aandacht voor en reflectie op het gebruik ervan.
Een voorbeeld hiervan is *predictive policing*. Dit is het gebruik van AI-gebaseerde modellen om efficiënt de inzet van de politie te informeren. De Nationale Politie experimenteerde hiermee in 2017 met het Criminaliteits Anticipatie Systeem (CAS), maar uit de pilot bleek dat het systeem leidde tot een zichzelf-vervullende voorspelling. Hoe meer politie er werd ingezet in een bepaald gebied, hoe meer misdaad er werd opgespoord in dat gebied, wat zorgde voor een vooringenomenheid in de dataset waar het systeem zich op baseerde. Dit is een voorbeeld van een systeem wat destijds voldeed aan wet- en regelgeving, en toch maatschappelijk onwenselijke gevolgen had.

2.2 RISICOMANAGEMENT

De Algemene Rekenkamer ontwikkelde een Toetsingskader Algoritmes, waarin specifiek wordt benoemd welke integriteitsrisico's nieuw zijn door de digitale werkomgeving. Het toetsingskader formuleert vragen rondom de vijf belangrijkste risicogebieden: sturing en

verantwoording, model en data, IT-beheer en ethische uitdagingen. Digitale middelen maken vaak gebruik van persoonsgegevens. Daarom is het ook belangrijk om zicht te hebben op privacy.[4] Daarnaast is DPIA (Autoriteit Persoonsgegevens) ieen instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. Organisaties die een hoog **privacyrisico** lopen bij de verwerking van persoonsgegevens, zijn verplicht een DPIA te doen.[5] De PriSA (Centrum Informatiebeveiliging en Privacybescherming) is een managementtool om inzicht te krijgen in het volwassenheidsniveau van de organisatie bij het voldoen aan de **AVG**.[6] Met CapAI (Oxford University) kan een organisatie nagaan in hoeverre zij handelen in lijn met de **Europese wetgeving** over AI. Het Belgische Kenniscentrum voor Data en Maatschappij heeft een verzameling van soortgelijke tools, waaronder een kaartspel waarmee **blindspots in zelflerende algoritmes** herkend kunnen worden en een ethisch logboek om integere besluitvorming te bevorderen.[7]

2.3 ACTUALISEREN INTEGRITEITSBELEID

Door de snelle ontwikkeling van digitale middelen is het integriteitsbeleid van organisaties en het gebruik van die middelen nog niet overal met elkaar in overeenstemming. Doe dit zo snel mogelijk. Dit is belangrijk om de ethische vraagstukken die innovaties met zich brengen te beantwoorden en gemaakte keuzes verdedigen. Het beschermt de organisatie en de mensen die erin werken. Ontwikkel eerst een heldere visie op het ethisch gebruik van digitale middelen, zodat niet iedere innovatie die nog volgt vraagt om beleidsaanpassing.

Ga voor informatie over ethisch gebruik van digitale middelen en inspiratie naar de e-learnings van de Rijksorganisatie voor Ontwikkeling, Digitalisering en innovatie.

[4] Het toetsingskader is ontworpen voor auditors (controleurs en toezichthouders). Voor meer informatie, zie ook de website van de Algemene Rekenkamer: https://www.rekenkamer.nl/onderwerpen/a/algoritmes/toetsingskader

[5] Voor meer informatie, zie ook de website van de Autoriteit Persoonsgegevens: https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/data-protection-impact-assessment-dpia

[6] Voor meer informatie, zie ook de website van het Centrum Informatiebeveiliging en Privacybescherming: https://www.cip-overheid.nl/

[7] Let op, het Kenniscentrum voor Data en Maatschappij is een Belgisch kenniscentrum, waardoor de exacte toepassing van de tools kan verschillen in het licht van Nederlandse wet- en regelgeving.

3. DE ZEVEN ONDERDELEN VAN INTEGRITEIT

Naast de tools uit het vorige hoofdstuk, biedt het Huis handvatten aan voor het actualiseren van integriteitsbeleid aan de hand van de zeven pijlers van integriteitsinfrastructuur. De tips geven aandachtspunten mee voor het integer gebruik van digitale middelen. De vragen kunnen organisatiebreed gebruikt worden om het gesprek over een integere digitale werkomgeving en integer gebruik van digitale middelen op gang te brengen.

3.1 LEIDERSCHAP EN STRATEGIE

Leidinggevenden zijn verantwoordelijk voor het integer gebruik van digitale middelen in hun organisatie. Onder **ethisch leiderschap** valt het bevorderen van integer gebruik van digitale middelen. Het is van belang dat leidinggevenden richting geven aan het integer gebruik van de digitale systemen waarmee een organisatie werkt. Daarnaast is het van belang dat leidinggevenden nadenken over strategische organisatiebeslissingen op digitaal vlak. Welke digitale middelen gebruikt de organisatie? Met welk doel worden deze middelen ingezet? Voor ethisch leiderschap is het belangrijk om na te gaan of de efficiëntie van de inzet van digitale middelen opweegt tegen mogelijke negatieve effecten van de technologie. Het is daarnaast belangrijk dat de directie toezicht houdt op het gebruik van digitale middelen in de organisatie (zie daarvoor ook *3.5 Melden en handhaven* in deze brochure). In een grotere organisatie kan een CIO daarbij een stevige rol vervullen.

Medewerkers hebben soms beperkt zicht op hoe zij integer gebruik kunnen maken van de digitale systemen in de organisatie. Daarom is het belangrijk om te investeren in de **digitale geletterdheid** in de organisatie en een kritisch gesprek te faciliteren over wat het integer gebruiken van technologie inhoudt. Een gebrek aan digitale geletterdheid kan een extra impuls zijn voor de directie om een duidelijke visie te formuleren op het gebruik van digitale middelen.

Het werken in verschillende digitale systemen vraagt flexibiliteit en lerend vermogen van werknemers. Dit geldt ook voor leidinggevenden: **voorbeeldgedrag** is in de omgang met digitale middelen noodzakelijk. Het is voor werknemers niet altijd helder hoe digitale systemen werken en welke integriteitsrisico's het gebruik van digitale middelen met zich meebrengen. Ook draaien steeds meer digitale tools (gedeeltelijk) op AI-toepassingen, waardoor sommige beslissingen in een werkproces worden uitbesteed aan technologie. Dit zorgt voor efficiëntere werkprocessen, maar heeft als belangrijk nadeel dat het moeilijker is om na te gaan waar de verantwoordelijkheid voor de uitkomsten van bepaalde werkprocessen ligt.

Daarnaast gaan de ontwikkelingen op digitaal gebied snel, terwijl wetgeving soms achterblijft. Dit bemoeilijkt sturing op integer gebruik van digitale middelen. Het is van belang om normstellend op te treden wat betreft integer gebruik van digitale middelen, zoals het opstellen van een waardengeoriënteerde **gedragscode** met aandacht voor de nieuwe vragen en dilemma's die digitale middelen met zich meebrengen. Dan weten medewerkers waar zij aan toe zijn. Enkel een gedragscode is vaak niet genoeg: in een organisatie moet er ruimte zijn om met elkaar doorlopend te bespreken wat wel en niet wenselijk gebruik is van digitale middelen, en van elkaar te leren.

3.1.1 TIPS

1. Bied werknemers **duidelijkheid** op het gebied van integer werken met digitale middelen.
2. Zorg voor aandacht voor digitale middelen in het **integriteitsbeleid** van de organisatie en borg de actualisering van dit beleid.
3. Maak een **risicoanalyse** en zorg voor **beschermingsmaatregelen** voor het gebruik van digitale middelen voor het actualiseren van het integriteitsbeleid van de organisatie. Hiervoor kunt u de vragen in deze brochure gebruiken. Daarnaast biedt het Huis ook een lijst met behulpzame tools in hoofdstuk 2 van deze brochure.
4. Wees bewust van het feit dat de organisatie nog niet blind kan varen op de output van AI-toepassingen. Door de snelle veranderingen moeten medewerkers **alert zijn op onverwachte fouten en uitkomsten**.

3.1.2 AANDACHTSPUNTEN

1. Welke **visie** over integer gebruik van digitale middelen wordt er door de directie uitgedragen? Hoe ziet een integere digitale werkomgeving in de organisatie eruit? In hoeverre wordt de visie op een integere digitale werkomgeving meegenomen in het integriteitsmanagement van de organisatie?
2. Wat is de mate van **afhankelijkheid** van digitale middelen in de werkprocessen van de organisatie?
3. Met welk **doel** zet de organisatie digitale middelen in?
4. In hoeverre worden er organisatiebrede **gesprekken** gevoerd over integere omgang met of de inzet van digitale middelen? Is er **draagvlak** onder de medewerkers voor het gebruik van bepaalde digitale middelen?

3.2 WAARDEN EN NORMEN

Ook als een organisatie zich aan geldende wet- en regelgeving houdt, kan er door gebruik van digitale middelen schade worden berokkend. Daarom is het belangrijk om stil te staan bij de waarden en normen rondom de inzet en het gebruik van digitale middelen. Deze waarden en normen geven invulling aan wat integer handelen inhoudt en helpen bij het maken van weloverwogen beslissingen. De waarden en normen van een organisatie worden beschreven in de gedragscode, en blijken vaak ook uit visie- en missiestukken van een organisatie. Deze code geeft richting aan de cultuur in een organisatie en schrijft voor hoe medewerkers zich dienen te gedragen. Het actualiseren van de gedragscode kan medewerkers helpen in het maken van integere beslissingen in het gebruik van digitale middelen.

Digitale middelen lijken objectieve processen die effectief en efficiënt neutrale resultaten voortbrengen, maar dit is niet altijd zo. AI-toepassingen presenteren informatie op een overtuigende wijze, terwijl deze soms feitelijk onjuist of niet betrouwbaar is. Dit zorgt voor schijnzekerheid.

Bij de ontwikkeling van digitale middelen worden bepaalde waarden centraal gesteld, waardoor blinde vlekken kunnen ontstaan. Die blinde vlekken kunnen negatieve gevolgen hebben. Digitale middelen met AI-toepassingen kunnen onbedoeld vooringenomenheid versterken, met ongewenste gevolgen zoals uitsluiting en discriminatie.

Voorbeeld
Een voorbeeld van het versterken van vooringenomenheid met AI-middelen is de recruiteringstool die een Amerikaanse bedrijf gebruikte in het selecteren van CV's tussen 2014 en 2017. Deze tool was bedoeld om zo efficiënt mogelijk CV's te selecteren om kandidaten uit te nodigen op gesprek. De tool baseerde zich op sollicitatie-data van de tien jaar voorafgaand aan de ingebruikneming van de tool. Bij technische functies waren in die periode mannen oververtegenwoordigd ten opzichte van vrouwen en deze bias werd overgenomen in de dataset waar de recruteringstool zich op baseerde. Dit resulteerde in de uitsluiting van vrouwelijke sollicitanten door de tool.

Er kan vooringenomenheid zitten in het ontwerp van de digitale middelen, in de data die door digitale systemen worden verzameld, verwerkt of toegepast en vooringenomenheid in de output van die digitale systemen. Deze vooringenomenheid wordt veroorzaakt door foutieve aannames in de gebruikte datasets, de gebruiker van de digitale middelen of in de ontwikkelaar van de software. Als medewerkers zich niet bewust zijn van deze vooringenomenheid en deze niet wordt gecorrigeerd, kan dit negatieve gevolgen hebben. Het is niet mogelijk om volledig zonder vooringenomenheid te werken, en daarom is het belangrijk om in het gebruik van digitale middelen ons bewust te zijn van de risico's.

Het is van belang om alert te blijven op of de uitkomsten van digitale middelen nog in lijn zijn met de waarden van de organisatie. Veel routinematige processen worden geautomatiseerd, waardoor het kan voorkomen dat fouten, vooroordelen of onbedoelde effecten (bijvoorbeeld in zelflerende algoritmes) onopgemerkt blijven en herhaald worden. Dit kan ondervangen worden door voldoende menselijke controle in te bouwen in werkprocessen. Ook helpt een menselijke blik om nuances en context te bewaren, wat in het bijzonder belangrijk is als werkprocessen mensen direct raken.

3.2.1 TIPS

1. Neem integer gebruik van digitale middelen op in de **gedragscode**. Beschrijf hier bijvoorbeeld of/hoe medewerkers moeten omgaan met AI-toepassingen als generatieve AI-chatbots zoals Chat GPT.
2. Wees in processen van verantwoording **transparant** over de inzet van digitale middelen en hun werking.[8]
3. Beperk AI-gebruik in gevallen waar **menselijke toetsing** wenselijk is, gelet op de maatschappelijke impact van het gebruik van AI.

3.2.2 AANDACHTSPUNTEN

1. Hoe **relevant** en **representatief** is de input van digitale middelen? Heeft uw organisatie de data op orde?
2. In hoeverre zijn medewerkers bekend met het risico van **vooringenomenheid** in hun eigen gebruik van digitale middelen en de digitale systemen waarmee zij werken?
3. In hoeverre is er sprake van **menselijke toetsing** bij het nemen van beslissingen op basis van input van het AI-systeem en hoe worden medewerkers in staat gesteld om die rol te spelen?
4. Hoe zijn de **organisatiewaarden** afgelopen tijd veranderd? Worden deze waarden nog weerspiegeld in de keuze voor en de omgang met de digitale middelen die de organisatie gebruikt?

[8] Het is momenteel niet verplicht om uw algoritmes bekend te maken, maar die verplichting komt er wel aan voor overheidsorganisaties. Voor meer informatie hierover, zie: https://algoritmes.overheid.nl/nl/footer/over

3.3 STRUCTUREN EN PROCEDURES

Bij gebruik van digitale middelen is het belangrijk om heldere werkprocessen in te richten, waarin medewerkers op de hoogte zijn van de regels omtrent integer gebruik van digitale middelen. Hierbij is het van belang dat zij op de hoogte zijn van relevante wet- en regelgeving. Met een risicoanalyse gericht op integriteitsrisico's in het digitale domein kunnen werkgevers inzicht krijgen in de kwetsbaarheden van hun organisatie op digitaal vlak. Digitale middelen zijn in sommige werkprocessen onontbeerlijk geworden. Kan een organisatie nog functioneren zonder digitale middelen wanneer blijkt dat deze onwenselijk grote risico's met zich meebrengen? (zie voor deze laatste vraag ook hoofdstuk 3.1 Leiderschap en strategie)

Wet- en regelgeving in het digitale domein ontwikkelt zich snel. Daarom is het belangrijk om na te gaan of de structuren en procedures in de organisatie nog voldoen aan de meest recente wet- en regelgeving op gebied van digitalisering. Denk hierbij aan Europese richtlijnen voor databeveiliging om datalekken te voorkomen. Wanneer digitale middelen worden ingezet voor gegevensverzameling en -verwerking, dan moet de organisatie daarbij voldoen aan privacywetgeving, zoals de AVG. Soms biedt de wetgever organisaties een soepel wettelijk kader, de 'regelluwe ruimte', zodat zij kunnen experimenteren met het inzetten van nieuwe technologieën zonder dat zij moeten voldoen aan de hoge eisen van bestaande wet- en regelgeving.

3.3.1 TIPS

1. Digitale middelen kunnen integriteitsrisico's met zich meebrengen, gerelateerd aan specifieke functies binnen de organisatie. Actualiseer het **overzicht kwetsbare functies** op het gebruik van en toegang tot specifieke digitale systemen in de organisatie.
2. Ga na welk **risiconiveau** het **gebruik van AI** in de organisatie heeft volgens de AI Act. Kijk of de werkprocessen van de organisatie voldoen aan de eisen van deze Europese richtlijn en pas procedures in de organisatie daarop aan.
3. Houd er rekening mee dat overtredingen van **Europese wetgeving** als de AI Act zware boetes tot gevolg kunnen hebben.

3.3.2 AANDACHTSPUNTEN

1. Hoe kunnen medewerkers integer omgaan met **data** in de organisatie? Hoe zijn deze mogelijkheden verankerd werkprocessen?
2. Nodigt de huidige **inrichting** van de organisatie uit tot integer gebruik van digitale middelen? Denk hierbij bijvoorbeeld aan: hebben medewerkers alleen toegang tot documenten waartoe zij geautoriseerd zijn?
3. Hoe wordt er in de huidige procedures in de organisatie rekening gehouden met de **snelle veranderingen** in het digitale domein? Welke **controlemechanismen** zijn ingesteld om te voorkomen dat personen binnen of buiten de organisatie disproportioneel getroffen worden door het gebruik van digitale middelen?
4. Wat is de **wettelijke grondslag** voor de inzet van digitale middelen, met name van AI-systemen en de besluiten die deze systemen in de organisatie nemen?
5. Wat is de impact van het mogelijk uitvallen of disfunctioneren van digitale systemen? Welke integriteitsrisico's komen kijken bij het **niet-functioneren** van digitale middelen in de organisatie? In hoeverre is het mogelijk om te **stoppen** met het gebruik van bepaalde digitale middelen, mocht het systeem onwenselijke effecten of foutieve resultaten voortbrengen?

3.4 PERSONEEL EN CULTUUR

Digitale systemen met AI-toepassingen worden in toenemende mate ingezet door HR-afdelingen in organisaties. Digitale middelen worden gebruikt voor het automatiseren van HR-processen, zoals personeelvolgsystemen (werktijdregistratie, registratie ziekteverzuim) en werving- en selectieprocessen (CV-selectie, digitale assessments). Ook worden digitale middelen gebruikt voor het opsporen van onregelmatigheden en het monitoren van online gedrag van medewerkers. Hoewel al deze toepassingen het HR-proces efficiëntie en effectiviteit opleveren, worden deze toepassingen ook in verband gebracht met integriteitsrisico's. Ook kan de inzet van digitale technieken middels intensieve digitale monitoring van medewerkers zorgen voor gevoelens van wantrouwen en een negatieve sfeer in de organisatie.

Voorbeeld
AI-toepassingen kunnen uitkomsten vaak op een overtuigende manier presenteren, waardoor er in de organisatie schijnzekerheid kan ontstaan over de uitkomsten die digitale systemen genereren. In HR-context kan dit bijvoorbeeld leiden tot verkeerde aannames of beslissingen bij het beoordelen van een CV of het schrijven van een functioneringsverslag. In dat laatste geval kunt u denken aan een functioneringsverslag over een uitgevallen medewerker. Een AI-toepassing kan de context missen dat iemand is uitgevallen door ziekte of persoonlijke problemen, en een medewerker ten onrechte kwalificeren als 'niet functionerend'.

Daarnaast kan het aantrekkelijk zijn om de productiviteit van medewerkers te monitoren door digitale middelen, maar dit kan wantrouwen uitstralen en ongewenste gevolgen hebben. Een voorbeeld hiervan is het "Time Off Task"-systeem wat een Amerikaanse bedrijf gebruikte om de productiviteit van medewerkers te monitoren. De resultaten van dit systeem gebruikte het bedrijf om disciplinaire maatregelen op te leggen aan medewerkers bij wie de productiviteit volgens het systeem tegenviel, of als reden voor ontslag. Echter, het systeem was zo scherp afgesteld, dat ook wc-bezoeken, het praten tegen collega's en de weg kwijt zijn in het magazijn werden geclassificeerd als een gebrek aan productiviteit.

Het is belangrijk om medewerkers te betrekken in visievorming over een integere digitale werkomgeving, de keuze voor bepaalde digitale technieken en het gesprek over hoe digitale middelen ingezet worden in de organisatie. Op die manier krijgen medewerkers een beter begrip van de mogelijke (bij)effecten van de nieuwe digitale technieken waar een organisatie mee aan de slag gaat. Tot slot versterkt het de betrokkenheid en het draagvlak voor (verantwoorde) inzet van digitale middelen en (mogelijke) digitale innovatie in de organisatie.

3.4.1 TIPS

1. Wees bewust, ook al opereert de organisatie binnen de privacywetgeving, van het potentieel **uitstralen van wantrouwen** bij een te uitgebreide digitale monitoring van werknemers. Dit kan de organisatiecultuur op een negatieve manier beïnvloeden.
2. Wees bewust van het belang van **menselijke interactie** in HR-processen. Bij de inzet van digitale middelen moet er altijd ruimte zijn voor interactie en persoonlijke beoordeling. Bij beslissingen over mensen moeten HR-professionals de uiteindelijke afweging maken en daarbij moet rekening gehouden worden met de context.
3. Blijf aandachtig op **vooringenomenheid** bij gebruik van AI bij werving en selectie. Zorg er altijd voor dat AI niet de eindbeslissing maakt over uitnodigen van

sollicitanten en aannemen van nieuwe werknemers. Denk in het selectieproces ook na over de mogelijkheid van semi-anoniem solliciteren om discriminatie te voorkomen, waarbij sollicitanten hun leeftijd of foto niet hoeven op te nemen in hun CV.

4. Zorg voor **AI-geletterdheid** bij personeel. Volgens Europese wetgeving moeten medewerkers die werken met AI-gebaseerde digitale systemen deze kunnen begrijpen, verantwoord toepassen en evalueren. Daarnaast is het belangrijk dat HR-functionarissen training krijgen in het kritisch beoordelen van uitkomsten van digitale middelen, omdat beslissingen over personeel niet zonder meer overgelaten kunnen worden aan digitale systemen.

3.4.2 AANDACHTSPUNTEN

1. Heeft de organisatie de benodigde **deskundigheid** binnen handbereik voor het integer gebruik van digitale middelen? Dit kan ook een externe partij zijn, zoals een IT-ondersteuner.
2. Hoe worden digitale middelen ingezet om interne onregelmatigheden op te sporen? Heeft deze inzet effect op de **organisatiecultuur**?

3.5 MELDEN EN HANDHAVEN

Wanneer een digitaal systeem niet binnen de waarden en normen van een organisatie opereert, kan het grote schade aanrichten. Dit is met name het geval wanneer het systeem een centrale plek heeft in de werkprocessen van een organisatie, of een groot volume aan data verwerkt. Als een medewerker misbruik maakt van een digitaal systeem, kan dit ook grote negatieve gevolgen hebben. Daarom is het belangrijk dat incidenten vroeg worden gesignaleerd en serieus worden opgepakt. Iedereen binnen de organisatie moet alert zijn op mogelijke misstanden rondom niet-integere inzet en gebruik van digitale systemen, en de waardering voelen om problemen op dit gebied te bespreken of te melden. Dit vraagt van medewerkers dat zij integriteitsschendingen snel signaleren en van werkgevers dat zij bij een melding snel handelen, en handhaven als er regels overschreden worden. Het gebruik van digitale middelen moet plaatsvinden binnen de gestelde kaders. Moedwillig negeren van die kaders moet leiden tot arbeidsrechtelijke gevolgen.

Voorbeeld
Een datalek is niet altijd even makkelijk te herkennen. Een medewerker merkt dat een collega gevoelige klantdata via een openbare Cloudmap heeft gedeeld. Een IT-technicus stelt een database met klantgegevens tijdelijk open voor externe toegang om een systeemfout te testen, maar vergeet deze later weer te sluiten. Een medewerker vindt een onbeveiligd USB-stick met gevoelige projectgegevens in de koffiehoek.

3.5.1 BELANGRIJKSTE ONTWIKKELINGEN

Door de inzet van digitale middelen is het in toenemende mate makkelijker om ongeregeldheden op te sporen. Denk hierbij aan het monitoren van uitgaande mails om het lekken van gevoelige informatie op te sporen. Digitale systemen kunnen zo ingericht worden, dat niet-integer gebruik door medewerkers snel gesignaleerd en opgepakt kan worden.

Bij de inzet van digitale middelen voor opsporing van onregelmatigheden moeten de belangen van alle betrokken partijen worden meegewogen en is scherpe controle op proportionaliteit van de inzet van groot belang. Ook mogen organisaties bij signalen van

onregelmatigheden niet in alle gevallen zelf opvolging geven, maar kan het zijn dat handhaving moet plaatsvinden door politie, justitie, een inspectiedienst of toezichthouder.

Indien er in werkprocessen gebruik wordt gemaakt van digitale middelen met AI-toepassing, kan het voorkomen dat er een foutief besluit wordt genomen waarbij het onduidelijk is wie er verantwoordelijk is. Bijvoorbeeld bij een onterechte afwijzing, of een discriminerende beoordeling. Soms is er juridische onduidelijkheid over aansprakelijkheid, of is het onduidelijk of het een systeemfout betreft of een fout van de gebruiker van een digitaal middel. Daarom is het belangrijk om duidelijke afspraken te maken over wie er toezicht houdt op het gebruik van digitale middelen en het informeren van medewerkers als zij in algemene zin gevolgd worden.

Voorbeeld
Bij het gebruiken van *agentic* AI-toepassingen[9] is het niet altijd duidelijk wie er verantwoordelijk is als er dingen misgaan. Denk hierbij aan een zelfrijdende auto. Wie is aansprakelijk als deze auto een aanrijding veroorzaakt?

3.5.2 TIPS

1. Denk bij het toepassen van digitale middelen omtrent handhaving van regels na over **proportionaliteit** van de inzet en maak een **belangenafweging**. Dat iets technisch mogelijk is, betekent niet altijd dat het wenselijk is. Informeer medewerkers hierover.
2. Biedt medewerkers de mogelijkheden om twijfels en zorgen over digitale middelen te melden. **Neem bezorgdheden serieus**, behandel ze op een gepaste manier en gebruik signalen als input voor de evaluatie van digitale middelen in werkprocessen.
3. Bepaal wie wanneer gemachtigd is om te handhaven bij niet-integer gebruik van digitale middelen. Leg dit vast in de **meldprocedure** en het **onderzoeksprotocol**.

3.5.3 AANDACHTSPUNTEN

1. AI is aantrekkelijk om werkprocessen en procedures efficiënter te maken, maar voor het onderzoeken van integriteitsschendingen en misstanden is voorzichtigheid geboden. Het is belangrijk om kritisch te zijn welke **datasets** AI gebruikt om aanbevelingen te doen over mogelijke integriteitsschendingen. Ook is er het gevaar van een **zichzelf-vervullende voorspelling** bij het gebruik van AI voor handhaving. Zie ook het voorbeeld hierover in hoofdstuk 2.1 van deze brochure.
2. Om zich (digitaal) integer te kunnen gedragen, moeten werknemers op de hoogte zijn van de regels omtrent het gebruik van digitale middelen. Deel met medewerkers hoe er gehandhaafd wordt op niet-integer gebruik van de digitale werkomgeving. Weten medewerkers hoe zij de digitale systemen van een organisatie kunnen gebruiken op een manier die negatieve bijeffecten, zoals discriminerende besluiten, voorkomt?
3. Zijn medewerkers bekend met de meldprocedure rondom het melden van niet-integer gebruik van digitale middelen? Weten zij dat zij hier ook gebruik van mogen maken voor het melden van misstanden die ontstaan door niet-integer gebruik van digitale middelen? In hoeverre voelen medewerkers zich vrij om zorgen en twijfels over de inzet en het gebruik van digitale middelen te delen? Hoe wordt er in de organisatie gevolg gegeven aan deze zorgen?

[9] *Agentic* AI toepassingen zijn digitale middelen waarin autonome digitale systemen processen zelf coördineren.

3.6 COMMUNICATIE EN VERANTWOORDING

Open communicatie bij de inzet van digitale middelen is belangrijk voor het vertrouwen in de organisatie, zowel van medewerkers als externe belanghebbenden. Digitale innovaties gaan snel en kunnen ervoor zorgen dat processen van evaluatie en verantwoording onder druk staan. Terwijl het juist heel belangrijk is om de inzet van digitale middelen te evalueren en bevindingen terug te koppelen naar medewerkers en stakeholders. Dit is van belang, omdat bij het gebruik van digitale middelen terechte bezwaren kunnen ontstaan. Bijvoorbeeld omdat een gedeelte van menselijke beslissingen wordt uitbesteed aan technische toepassingen, waardoor het risico op foutieve beslissingen onverantwoord hoog is. Het is voor belanghebbenden belangrijk om na te kunnen gaan of een dergelijke beslissing voldoende rekening houdt met hun rechten en belangen en in lijn is met de waarden en normen van de organisatie.

3.6.1 TIPS

1. Communiceer de **reden voor de inzet** van digitale middelen en licht de **belangenafweging** toe die hierin is gemaakt. Benoem dilemma's en risico's. Dit kunt u makkelijker doen wanneer u als directie de organisatievisie op het gebruik van digitale middelen deelt met uw medewerkers.
2. Zorg bij de inzet van digitale middelen in werkprocessen voor heldere afspraken over **evaluatie** en **verantwoording** aan de relevante actoren.
3. Wees waar mogelijk **transparant** over de inzet van AI-toepassingen. Leg uit welke gegevens de digitale techniek gebruikt en hoe het AI-algoritme beslissingen neemt. Dit kan bijvoorbeeld door net als een privacyverklaring, ook een AI-verklaring op te nemen op jouw website.
4. De uitleg over de werking en het doel van het inzetten van digitale middelen moet **betekenisvol** zijn. Maak de uitleg begrijpelijk en let hierbij op verschillen in kennis en vaardigheden van gebruikers van de digitale middelen.
5. **Communiceer open** als er iets misgaat bij de inzet van digitale middelen. Benoem wat er is misgegaan, waarom de techniek gebruikt wordt (en of deze nog wordt gebruikt) en wat er wordt gedaan om te voorkomen dat de fout nog een keer gemaakt wordt.

3.6.2 AANDACHTSPUNTEN

1. In hoeverre zijn de digitale middelen die worden gebruikt **betrouwbaar**, **uitlegbaar** en **doelgericht**?
2. In hoeverre is het **doel** van de inzet van specifieke digitale middelen gecommuniceerd met gebruikers en andere belanghebbenden?
3. In hoeverre is de **data governance** op orde? Denk hierbij aan wie er toegang heeft tot data, of er integer gebruik wordt gemaakt van de beschikbare data en of er veilig gebruik wordt gemaakt van de data.
4. Hoe en door wie wordt het gebruik van digitale middelen **gecontroleerd**? En hoe en door wie wordt er **verantwoording** afgelegd over het integer gebruik van digitale middelen?

3.7 SAMENHANG EN BORGING

Vele gebruiksvormen van digitale middelen raken aan het integriteitsmanagement van een organisatie: denk bijvoorbeeld aan personeel volgsystemen, informatiehuishouding in de Cloud en het automatiseren van klantcontact met chatbots. Digitale systemen zijn vaak onderdeel van het merendeel van de werkprocessen in een organisatie. Daarom moet er niet alleen gekeken worden naar de losse integriteitsrisico's per digitaal middel dat een organisatie gebruikt, maar juist naar het geheel aan digitale middelen. Als er een overzicht is van de verschillende digitale middelen en systemen die een organisatie

gebruikt, kan er ook een inschatting gemaakt worden welke integriteitsrisico's die systemen in combinatie met elkaar met zich mee brengen.

Integriteitsbevordering in het gebruik en de inzet van digitale middelen vereist permanente aandacht in een organisatie. Naast dat er in samenhang gekeken moet worden naar de verschillende onderdelen van de digitale werkomgeving, is het ook van belang dat integer gebruik van digitale middelen een doorlopend onderwerp van gesprek is in de organisatie. Dit kan door het thema integriteit een vast onderdeel te maken in het evalueren van werkprocessen. Daarnaast kan een organisatie de aandachtspunten zoals beschreven in deze handreiking gebruiken voor organisatiebrede gesprekken over integer gebruik van digitale middelen.

Digitale middelen zijn onderdeel van de bedrijfsvoering en veranderen rap door digitale innovatie. Een organisatie die innoveert, moet zich herhaaldelijk afvragen welk effect een bepaalde innovatie heeft op de waarden van een organisatie. Het is belangrijk om zicht te hebben of een innovatie deze waarden versterkt of juist aantast. Hier krijgt een organisatie zicht op door monitoring onderdeel te maken van zowel de implementatie als het gebruik van digitale middelen. Het is belangrijk om in die monitoring de feedback van andere betrokken partijen te verwerken. Een organisatie moet er voor zorgen dat regelmatig wordt gecontroleerd of de bestaande regels en procedures nog up-to-date zijn en dat ze worden aangepast waar nodig.

3.7.1 TIPS

1. Richt een **plan-do-check-act cyclus** in. Met name het controleren van (zelflerende) algoritmes is van belang. Dit verkleint het risico dat er vooroordelen in het systeem sluipen.
2. Stel in grotere organisaties een **centrale coördinator** voor digitale middelen aan. Samen met de integriteitsfunctionaris en ICT-experts kan deze coördinator ervoor zorgen dat digitale middelen op een integere manier worden ingezet. In kleinere organisaties kan het coördineren van het integer gebruik van digitale middelen worden belegd bij degene die verantwoordelijk is voor het integriteitsbeleid.

Voorbeeld
Een goed voorbeeld dat het belang van controle op zelflerende algoritmes onderstreept, is de Toeslagenaffaire. In die casus slopen er vooroordelen in de digitale systemen die de Belastingdienst, het UWV en DUO gebruikten om fraude op te sporen, waardoor er een groot maatschappelijk misstand ontstond.

3.7.2 AANDACHTSPUNTEN

1. Hoe is de aandacht voor integer gebruik van digitale middelen geborgd in **evaluatieprocessen**?
2. Is er in het integriteitsbeleid van de organisatie aandacht voor de verschillende onderdelen van de digitale werkomgeving, en de specifieke dilemma's die deze onderdelen met zich meebrengen?

TOT SLOT

Om de kansen die digitale ontwikkelen bieden optimaal te benutten, is het van belang dat jouw organisatie zorg draagt voor een integere digitale werkomgeving. Niet alles wat mogelijk is, is ook wenselijk vanuit integriteitsperspectief. Het is belangrijk om in alle onderdelen van het integriteitsmanagement van jouw organisatie aandacht te hebben voor de weging van voor- en nadelen bij het gebruik van digitale middelen In een integere digitale werkomgeving is er aandacht voor de complexe wet- en regelgeving omtrent digitale technologieën en ook voor de ethische omgang met de veelheid van digitale middelen die een organisatie tot haar beschikking heeft. Extra aandacht moet uitgaan naar het belang van menselijke controle op processen die afhankelijk zijn van digitale technologie, het maken van een waarden- en belangenafweging in het gebruik van digitale middelen en oog voor de maatschappelijke risico's van digitale middelen die gebruik maken van AI. Hierbij is het van belang dat jij het integriteitsbeleid van jouw organisatie regelmatig actualiseert. De zeven onderdelen van de integriteitsinfrastructuur van het Huis voor Klokkenluiders kunnen hierbij helpen.

WILT U MORGEN AL AAN DE SLAG MET DEZE BROCHURE?

Dat kan op drie manieren:[10]

1. *Organiseer een kort overleg met sleutelfiguren*

Het doel van dit overleg is op korte termijn **draagvlak creëren** en **prioriteiten stellen**. Nodig de directie, HR, ICT en de integriteitsfunctionaris (of -coördinator) uit voor een kort overleg. Bespreek hierin:

- Welke digitale middelen (bijvoorbeeld AI, monitoring en data-analyses) worden er nu door de organisatie gebruikt?
- Wat zijn de grootste risico's of zorgen die medewerkers en leidinggevenden nu ervaren op gebied van digitale middelen?
- Welke visie heeft de directie op integer digitaal werken?

Het resultaat is een lijstje met 2-3 urgente aandachtspunten voor de korte termijn en een visie van de directie op integer gebruik van digitale middelen.

2. *Start met heldere communicatie naar alle medewerkers*

Het doel van dit actiepunt is de **bewustwording** onder medewerkers vergroten en **transparantie** bevorderen. Stuur een korte mail of bericht naar alle medewerkers met:

- Een korte uitleg waarom integer digitaal werken belangrijk is voor de organisatie en wat de visie van de organisatie is op het integer gebruik van digitale middelen.
- Een overzicht van de bestaande regels (bijvoorbeeld uit de gedragscode) en waar medewerkers deze regels kunnen raadplegen.
- Een oproep om zorgen en vragen te melden bij een aanspreekpunt (bijvoorbeeld HR of de integriteitscoördinator).
- Een aankondiging van een korte training of Q&A-sessie over dit onderwerp (zie actiepunt 3).

Het resultaat hiervan is dat medewerkers weten dat het onderwerp binnen de organisatie leeft en weten waar ze terecht kunnen met vragen.

[10] Als experiment is voor deze vraag gerelateerd aan dit document Le Chat AI gebruikt.

3. *Plan een korte, praktische training of workshop in over integer gebruik van digitale middelen*

Het doel van deze workshop of korte training is het **direct verbeteren van de kennis** en **vaardigheden** van medewerkers over integer omgaan met digitale middelen in de organisatie. Organiseer deze sessie (tussen de 30 en 60 minuten) op korte termijn (bijvoorbeeld binnen twee weken) voor alle medewerkers, en richt deze op:

- De basisprincipes van integer digitaal werken (bijvoorbeeld omgang met AI, data en privacy).
- Herkenning van risico's (bijvoorbeeld vooringenomenheid in AI, datalekken en onbedoeld misbruik).
- Waar en hoe medewerkers twijfels of incidenten kunnen melden.

Zet voor deze workshop of training bijvoorbeeld een externe expert in of een interne ICT-medewerker die de basis van integer digitaal werken kan uitleggen. Zo'n workshop heeft als resultaat dat medewerkers zich gehoord voelen in hun zorgen over digitaal werken en weten wat er van hen verwacht wordt op gebied van integer gebruik van digitale middelen. Zo kunnen zij direct aan de slag.

Bonus: zet een kleine werkgroep op

Ook kan de organisatie ervoor kiezen om een kleine werkgroep op te zetten van 2-3 gemotiveerde werknemers uit verschillende afdelingen die op korte termijn met de volgende acties aan de slag gaan:

- Het evalueren van de uitkomsten van het overleg met sleutelfiguren en de korte training.
- Het doen van een voorstel voor een eerste update van het integriteitsbeleid (bijvoorbeeld een paragraaf over integer digitaal werken).
- Het opstellen van een lijst met veel gestelde vragen over integer digitaal werken voor op de intranetpagina.

Over het Huis voor Klokkenluiders
Het Huis voor Klokkenluiders is een organisatie die zich bezig houdt met alles rondom klokkenluiden en integriteit. Van advies tot hulp, van onderzoek tot preventie. Wilt u meer weten? Onze website is een bron van informatie voor zowel werkgever als werknemers en beleidsmakers. U kunt ons vinden op http://www.huisvoorklokkenluiders.nl.

Dit is een uitgave van het Huis voor Klokkenluiders.

Contactgegevens
Muzenstraat 89-91, 2511 WB Den Haag
Telefoon: 088-13 31 000
E-mail: mailto:info@huisvoorklokkenluiders.nl

www.huisvoorklokkenluiders.nl