Deontologische code

2 december 2020

District

Colofon

District09
Bedrijfsvoering, cel HR

Publicatiedatum
2 december 2020

Contact
hrm@district09.gent

Adres
District09
Bellevue 1, 9050 Ledeberg
09 266 09 00

Maatschappelijke zetel
Stadhuis, Botermarkt 1, 9000 Gent

Inhoud

Inleiding

Toepassingsgebied

Deze deontologische code geldt voor alle medewerkers tewerkgesteld bij het Autonoom Gemeentebedrijf District09. We interpreteren het begrip 'medewerkers' hier in ruime zin: interne medewerkers, externe consultants, stagiairs en interims en terbeschikkinggestelde medewerkers van Stad Gent.

De ICT-gedragsregels (luik III) zijn van toepassing op alle ICT-middelen die het Autonoom Gemeentebedrijf beschikbaar stelt of die gekoppeld zijn met de omgeving van het Autonoom Gemeentebedrijf en haar partners. Ook toestellen waarop informatie van of voor het Autonoom Gemeentebedrijf verwerkt wordt, moeten aan deze ICT-gedragsregels beantwoorden.

De deontologische code is openbaar en raadpleegbaar via de website www.district09.gent.

Wat is integriteit?

Integriteit gaat over de handelingen en beslissingen van jou als medewerker. Het is geen karaktereigenschap: integriteit gaat niet over wie je bent, maar wel over wat je doet.

Integer handelen op je werk houdt drie zaken in:
Je oefent je functie goed en zorgvuldig uit. Je houdt rekening met je verantwoordelijkheden en de normen en waarden van de organisatie.
Je houdt in je keuzes, beslissingen en gedrag voldoende rekening met de rechten, belangen en wensen van alle betrokkenen.
Je bent op de hoogte van de gedragsregels en past die toe.

Waarom is integriteit belangrijk?

Een lokale overheid speelt een ingrijpende rol in het leven van de burger of voor een bedrijf.

Een overheid beschikt immers over bevoegdheden die rechtstreeks het leven van een burger of de situatie van een bedrijf kunnen beïnvloeden: een vergunning verlenen of weigeren, een subsidie toekennen of intrekken, een belasting of retributie heffen, hulp verlenen of stopzetten…

Bovendien heeft een overheid toegang tot allerlei persoonlijke of vertrouwelijke gegevens van burgers, organisaties en bedrijven.

Daarom is het cruciaal dat burgers en bedrijven vertrouwen stellen in het Autonoom Gemeentebedrijf District09.

Om dat vertrouwen te winnen en te behouden, moet je als medewerker steeds integer handelen. **Integer handelen versterkt** het vertrouwen in de overheid. De democratische rechtstaat is voor haar functioneren afhankelijk van het vertrouwen van de burger.

Waarom is een deontologische code belangrijk?

Welke functie je ook hebt, voor je omgeving ben je het gezicht van het Autonoom Gemeentebedrijf District09. Zowel in je werk als in je privéleven. Je bent dus mee verantwoordelijk voor het vertrouwen van burgers en bedrijven in de organisatie.

De deontologische code helpt je hierbij en biedt je een houvast. Ze geeft je een aantal gedragsregels om integer te handelen. Ze beschermt je tegen mogelijke risico's, beschuldigingen en druk van buitenaf. En ze kan je inspireren om een goede basishouding te vinden bij al je handelingen en beslissingen.

Deze **deontologische code** gaat eerst in op '**goed medewerkerschap'**. Dat is een basishouding, een mentaliteit die al je handelingen en beslissingen kan leiden. Als je deze korte inspiratietekst volgt, handel je als een goede medewerker .

Daarna bevat de deontologische code een aantal **'gedragsregels'.** Deze zijn opgesplitst in een luik met **algemene gedragsregels** (luik II) en een luik met specifieke **ICT-gedragsregels** over hoe je integer en veilig moet omgaan met de ICT-middelen van het Autonoom Gemeentebedrijf (luik III). Dit zijn allemaal gedragsregels die elke medewerker minstens moeten toepassen. Zo weet jij wat er van jou verwacht wordt, en weten eindgebruikers, burgers en externe partijen wat ze kunnen verwachten, zodat zij daar rekening mee kunnen houden.

De deontologische code heeft daarmee ook een **beschermende** functie. Ze helpt je om risico's te herkennen, om weerstand te bieden aan verleidingen en aan valse of lastig weerlegbare beschuldigingen, en om druk van buitenaf te weerstaan. Die risico's hebben te maken met geld, macht, kennis(monopolie), afhankelijkheid, veiligheid, emotionele betrokkenheid, een dubbele pet … en zouden tot gevolg kunnen hebben dat je als medewerker misschien niet meer in volledige onafhankelijkheid (en dus in het algemeen belang) een beslissing kan nemen. De 'gedragsregels' helpen je bij al je handelingen en beslissingen, en beschermen je tegen vergissingen of misstappen door onwetendheid.

Maar het is onmogelijk om elke denkbare situatie op voorhand te voorzien. Bovendien wijzigen de omstandigheden voortdurend door nieuwe ontwikkelingen: nieuwe technologieën, nieuwe wetgeving, nieuwe trends… De 'gedragsregels' in de deontologische code kunnen daarom **niet op alle situaties een kant-en-klaar antwoord** bieden. Je moet dus **altijd zelf blijven nadenken** en je bewust blijven van wat het betekent om integer te

handelen. En wat het betekent om een ‘goede medewerker’ te zijn. Spreek hierover in geval van twijfel ook met je collega’s en leidinggevende.

Het spreekt voor zich dat de leidinggevenden een belangrijke voorbeeldfunctie hebben voor bewustwording en naleving van de deontologische code. Ze zijn hierop ook steeds aanspreekbaar.

Link naar de organisatiecultuur en waarden

Het integriteitsbeleid en goed medewerkerschap gaan ook hand in hand met onze organisatiecultuur. Het Autonoom Gemeentebedrijf District09 heeft dezelfde cultuurambitie en waarden als de Stad Gent.

De cultuurambitie van het Autonoom Gemeentebedrijf kan samengevat worden in 3 principes:

- meer mens – wij maken van onze organisatie een plaats waar mensen het belangrijkst zijn;
- meer oplossingen – wij denken en handelen vanuit het resultaat dat wij willen behalen en zoeken oplossingen waar mogelijk
- minder regels – waar het kan vereenvoudigen we onze werkwijze.

Dit is hoe we willen samenwerken en wie we willen zijn. Deze deontologische code omvat daarom geen opgesomde lijst van alle mogelijke regeltjes. Ze beschrijft welke verwachtingen er gelden voor iedere medewerker van het Autonoom Gemeentebedrijf. Elke medewerker heeft de verantwoordelijkheid om de principes van de deontologische code te respecteren en te vertalen naar zijn dagelijkse werking.

Om ons dagelijks te helpen om deze 3 principes waar te maken, stellen we 4 organisatiewaarden voorop:

- open,
- betrokken,
- creatief en
- doelgericht.

Deze waarden tonen waar wij voor staan en ze geven richting aan onze organisatiecultuur voor de komende jaren.

Luik I. Goed medewerkerschap

‘Goed medewerkerschap’ betekent dat men op jou kan rekenen. Je bent met andere woorden betrouwbaar. Je neemt je taken serieus, houdt je aan de afspraken en toont voorbeeldgedrag.

- Je oefent je opdrachten **plichtsgetrouw en op een correcte wijze** uit. Dat doe je met respect voor je organisatie en voor de bestaande wet- en regelgeving.
- Je werkt met je leidinggevende en collega’s loyaal, open en constructief samen aan de opdracht van het Autonoom Gemeentebedrijf. Je verzorgt de **best mogelijke dienstverlening aan de burger**.
- Je laat je leiden door het **algemeen belang**. Je houdt uiteraard rekening met de belangen van iedereen die een beroep op jou doet, maar verliest nooit het algemeen belang uit oog.
- Je gaat **respectvol** om met collega’s en burgers. Je discrimineert niet en verleent niemand een voorkeursbehandeling.
- Je gaat **zorgvuldig en verantwoordelijk** om met bevoegdheden, middelen (gelden, goederen, kennis) en informatie.
- Je neemt verantwoordelijkheid voor je eigen handelen. Je bent aanspreekbaar op je gedrag, en je spreekt anderen hierop aan. Dat gaat vaak verder dan het vasthouden aan officiële regels.
- Je bent in staat om **verleidingen te weerstaan** en, beter nog, te voorkomen dat je in verleidelijke situaties terecht komt.

Bovenstaande principes betreffen de bovengrens van moreel handelen. Dat wil zeggen: wat verwachten we van onze medewerkers, wat is daarbij het streefdoel? Welke principes verwachten we bij het handelen van de medewerkers van het Autonoom Gemeentebedrijf in het kader van hun functie? Deze principes noemen we “goed medewerkerschap”.

Daarnaast is het belangrijk om een morele ondergrens vast te leggen in de deontologische code. Dit wil zeggen: wat zijn de absolute minimumgrenzen die iedere medewerker van het Autonoom Gemeentebedrijf moet respecteren? Deze minimumgrenzen leggen we vast in de hiernavolgende gedragsregels.

Luik II. Algemene gedragsregels

1. Respectvol omgaan met anderen

Je behandelt iedereen op gelijkwaardige wijze en met respect

Je behandelt iedereen met respect. Dat betekent dat je de ander serieus neemt, naar elkaar luistert en fatsoenlijk met elkaar omgaat.

Je benadert iedereen steeds hoffelijk, vriendelijk en respectvol. Ook in moeilijke situaties en bij klachten blijf je steeds rustig en beleefd.

Je houdt ook rekening met ieders rechten en belangen. Dit betekent niet dat je het iedereen altijd naar de zin moet maken. Het betekent dat je geval per geval de verschillende belangen zorgvuldig afweegt om tot een goede beslissing te komen. Je respecteert daarbij wet- en regelgeving.

Als je respect toont voor burgers, krijgen ze meer vertrouwen in onze organisatie. Het geeft blijk van een goede dienstverlening. Met respect voor collega's en voor de leden van het bestuur, maak je samenwerking veel makkelijker.

Iedere vorm van discriminatie is verboden

Je laat je bij de uitoefening van je functie niet beïnvloeden door filosofische, politieke of religieuze overtuigingen, door seksuele geaardheid, geslacht, ras, herkomst of andere persoonsgebonden kenmerken.

Onze organisatie hanteert een nultolerantie tegenover discriminatie. Zo ondertekent iedereen bij indiensttreding de anti-discriminatieverklaring.

Iedereen in onze organisatie is uniek. Je werkt met mensen met een verschillende herkomst, levensovertuiging, politieke voorkeur, geslacht en seksuele geaardheid.

Je mag anderen nooit voortrekken, achterstellen, negeren, kwetsen of pesten omwille van die verschillen.

Je vermijdt ongewenste omgangsvormen en ongewenst gedrag

Je respecteert elkaars grenzen en stelt geen gedrag dat de ander als ongewenst ervaart. Spreek anderen aan op hun ongewenst gedrag, en steun collega's die er het slachtoffer van zijn. Toets ook voldoende of jij gepast hebt gereageerd.

Onder ongewenst gedrag verstaan we grensoverschrijdend gedrag, zoals verbaal of fysiek geweld, pesten en seksuele intimidatie.

Onder ongewenst seksueel gedrag verstaan we elke vorm van verbaal, niet-verbaal of lichamelijk gedrag van seksuele aard waarvan je weet, of zou moeten weten, dat het afbreuk doet aan iemands waardigheid.

Dit zijn enkele voorbeelden van ongewenst gedrag:

- roddelen over collega's;
- opzettelijk belangrijke informatie 'vergeten' door te geven;
- seksueel getinte opmerkingen;
- racistische 'grappen';
- een collega negeren of belachelijk maken;
- hacking ('inbreken' in iemands computer);
- stalking (iemand hinderlijk volgen of lastigvallen);
- spamming (ongevraagd grote aantallen e-mails of sms'en sturen);
- …

Het is belangrijk elkaars grenzen te kennen en die te respecteren, want bij ongewenste omgangsvormen speelt beleving een belangrijke rol. Wat de ene als grappig of vriendelijk woord of gebaar ziet, kan een ander als opdringerig of vervelend aanvoelen.

Voel je jezelf ongemakkelijk bij bepaalde opmerkingen of bij het gedrag van een collega? Blijf er niet mee zitten en bespreek dit met die collega. Je kan het ook bespreken met je leidinggevende of een vertrouwenspersoon.

Je geeft zelf het goede voorbeeld, spreekt anderen aan op hun ongewenst gedrag en steunt collega's die het slachtoffer zijn van ongewenste omgangsvormen. Ook al ben je niet zelf verantwoordelijk voor het pestgedrag, je bent er wel mee verantwoordelijk voor dat het stopt. Ook hiervoor kan je terecht bij je leidinggevende of een vertrouwenspersoon.

2. Belangenvermenging vermijden

Je maakt je niet schuldig aan belangenvermenging

Je mag je functie niet gebruiken om jouw eigen belangen te dienen. Je mag ze ook niet gebruiken voor de belangen van een ander(e organisatie) bij wie je persoonlijk betrokken bent, ook al staat daar geen wederdienst tegenover.

Burgers en externe partijen moeten erop kunnen vertrouwen dat de overheid niet bevooroordeeld of partijdig is, en dat ambtenaren zich niet laten leiden door eigenbelang of verkeerde motieven.

Het kan voor jezelf verleidelijk zijn om iets te doen dat in je eigen belang is of in het belang van een persoon of organisatie waar je je betrokken bij voelt. Soms kan een organisatie jou om iets vragen en je het gevoel geven dat je haar zou moeten helpen, terwijl ze daar eigenlijk geen recht op heeft.

Behandel nooit een dossier en wees terughoudend bij tussenkomst rond dossiers:

- waarbij je zelf betrokken bent;
- waarbij een vriend, familielid, bedrijf of vereniging waarin je actief bent, betrokken is; of
- van een persoon met wie je een conflict hebt.

Je vermijdt elke schijn van belangenvermenging

Je gaat uit jezelf de schijn van belangenvermenging en vriendjespolitiek tegen.

Ook ‘de schijn tegen’ is niet goed voor de geloofwaardigheid van en het vertrouwen in de overheid. De verdenking van belangenvermenging hoeft niet waar te zijn om het vertrouwen in de overheid te beschadigen. Al is het maar omdat het heel lastig uit te leggen is.

Je kan de schijn van belangenvermenging bijvoorbeeld tegengaan door je persoonlijk belang te melden aan je leidinggevende wanneer je een dossier van een naaste of bekende krijgt. Je leidinggevende kan dat dossier dan overdragen aan een collega.

Je maakt melding van een bijberoep en bent waakzaam bij nevenwerkzaamheden

Je mag vrijwilligerswerk doen, een bijberoep uitoefenen of een andere nevenactiviteit uitvoeren. Bespreek het wel op voorhand met je leidinggevende als je twijfelt of het verenigbaar is met je functie.

De term ‘nevenwerkzaamheden’ moet je ruim zien. Het kan gaan om het lidmaatschap van het bestuur van een vereniging, vrijwilligerswerk of een betaald bijberoep. Ook eenmalige activiteiten vallen hieronder, zoals een artikel schrijven of een lezing geven op een congres.

Als je een nevenwerkzaamheid of bijberoep hebt dat raakvlakken heeft met de uitoefening van je functie, is het risico op (schijn van) belangenvermenging groter. Bespreek dit daarom steeds met je leidinggevende.

Een nevenwerkzaamheid of bijberoep is normaalgezien geen probleem als ze:

- verenigbaar is met je functie,
- het vervullen van je ambtsplichten niet in de weg staat, en
- de waardigheid van het ambt en je eigen onafhankelijkheid niet in het gedrang brengt.

Je verricht je nevenwerkzaamheid of bijberoep steeds in je vrije tijd of tijdens verlof.

Soms word je vanuit je functie of expertise, uitgenodigd als gastspreker of als panellid in een debat, op een privé-event of commercieel georganiseerd congres. Een dergelijke samenwerking kan nuttig en wenselijk zijn, maar waak erover dat dit je onafhankelijkheid niet in het gedrang brengt.

Besef ook dat de organisatie streeft naar kennisdeling zonder dit te commercialiseren. Als je dienstvrijstelling krijgt om aan een dergelijke activiteit deel te nemen, mag je je hier niet voor laten betalen. Doe je dit in je vrije tijd of tijdens verlof, dan kan dat eventueel wel. Wees ook hier open en eerlijk over.

3. Corruptie tegengaan

Je maakt je niet schuldig aan corruptie

Je laat je niet omkopen voor geld, goederen of diensten. Je vraagt ook geen geld, goederen of diensten voor jouw werk of tussenkomst.

Corruptie is een strafbaar feit en dus verboden. Bij actieve corruptie vraag je als medewerker een betaling, een gift, een gunst of een ander voordeel om gewoon de wet of het beleid uit te voeren. Bij passieve corruptie neem je van anderen een betaling, een gift, een gunst of een ander voordeel aan om de wet of het beleid juist niet uit te voeren of bijvoorbeeld een voorkeursbehandeling te genieten. Elke poging meld je aan je leidinggevende.

Je mag als medewerker je macht of invloed nooit gebruiken in je eigen voordeel. Corruptie beschadigt het vertrouwen van de burger of organisaties, zelfs al gaat het om iets heel kleins.

Dit zijn enkele voorbeelden van pogingen tot corruptie:

- Iemand biedt jou geld, een geschenk, faciliteiten of diensten aan om voorrang te krijgen in behandeling. Bijvoorbeeld sneller een plaats in een woonzorgcentrum.
- Iemand biedt jou geld, een geschenk, faciliteiten of diensten aan om iets te krijgen waar hij geen recht op heeft. Bijvoorbeeld een vergunning, of een toelage.

- Je benadert als medewerker zelf een persoon of een partij om geld of een gunst te krijgen, in ruil voor het gebruik van jouw positie of invloed. Bijvoorbeeld om niet handhavend op te treden.
- Je perst burgers af en vraagt hen geld of gunsten om hun vergunning of document te krijgen.

Pas als je de aangeboden voordelen ook effectief aanvaardt, is er sprake van corruptie.

Je vermijdt elke schijn van corruptie

Je gaat uit jezelf de schijn van corruptie tegen.

Je moet als medewerker alles doen wat je kunt om ook de schijn van corruptie te vermijden. Ook de schijn van corruptie is vernietigend voor de geloofwaardigheid van en het vertrouwen in het Autonoom Gemeentebedrijf. En het kan jezelf in moeilijkheden brengen.

Spreek met je leidinggevende duidelijk af wanneer je geschenken en voordelen (uitnodigingen, faciliteiten, diensten, etentjes, reizen …) aanneemt en wanneer je ze afwijst. Zorg dat je altijd naar zo'n afspraak kunt verwijzen als iemand je vraagt waarom je een aanbod aanneemt of afwijst.

Je neemt niet zomaar geschenken aan die je in je functie krijgt aangeboden

Je neemt geen geschenken aan die je in je functie krijgt aangeboden. Zo wek je nooit de schijn dat je je daardoor laat beïnvloeden. Een geschenk van geringe waarde kan je soms wel aannemen als weigeren kwetsend is én de schijn van corruptie zeer klein is. Bespreek dat dan steeds met je leidinggevende.

Een geschenk krijg je altijd omdat je een bepaalde functie hebt. Zelfs de geschenken van weinig waarde of de geschenken uit goede bedoelingen.

Als je een geschenk aanneemt, kan de schijn worden gewekt dat je je daardoor laat beïnvloeden. Denk dus goed na over wie jou op welk moment iets aanbiedt, en wat daar de achtergrond van kan zijn. Een bedankje na een geslaagd evenement, kan soms een gewone beleefdheidsuitwisseling zijn en zonder bijbedoelingen gebeuren. Maar krijg je datzelfde bedankje van iemand die meedingt in een aanbestedingsprocedure? Dan is de schijn van corruptie veel groter.

Maak zelf actief en vooraf duidelijk dat je geen geschenken aanneemt, noch op het werk, noch thuis. Zo zorg je dat je niet in een lastige situatie komt en iemand moet beledigen of voor het hoofd stoten..

Alleen als weigeren kwetsend is of anderen in verlegenheid brengt én als de schijn van corruptie minimaal is, kan je een uitzondering maken. In dat geval kun je soms een geschenk van geringe waarde aanvaarden, zoals een bos bloemen, een doos pralines of een fles wijn. Bespreek dit in team of met je leidinggevende. Samen kijk je wat er met het geschenk gedaan wordt.

Je bespreekt uitnodigingen steeds met je leidinggevende

Als het past binnen je functie, mag je ingaan op uitnodigingen voor lunches, diners, recepties, (buitenlandse) dienstreizen of andere evenementen. Bespreek het wel op voorhand met je leidinggevende, en kijk of het wel past binnen de omstandigheden.

Netwerken kan deel uitmaken van je functie. Bij dat netwerken krijg je soms uitnodigingen van externe partijen voor lunches, diners, recepties of andere evenementen. Daar mag je eventueel op ingaan, maar ga er verstandig mee om. De uitnodiging moet functioneel en doelmatig zijn en mag niet buitensporig zijn.

Ook de context waarbinnen de uitnodiging plaatsvindt is van belang. Een zakelijke bespreking combineren met een gewoon etentje, is meestal geen probleem. Maar een uitnodiging in een sterrenrestaurant of in de viplounge bij een evenement, wekt meestal wel de schijn op dat je je laat beïnvloeden. Zeker als de uitnodiging komt van een bedrijf dat kandidaat is voor een opdracht.

Belangrijk is dat je je onafhankelijkheid bewaakt en jezelf niet uitgebreid laat trakteren. Daarom bespreek je uitnodigingen steeds met je leidinggevende.

Laat mogelijke klanten of leveranciers nooit reis-, verblijfs- of hotelkosten betalen voor jou wanneer er een schijn van corruptie mogelijk is. Je bespreekt uitnodigingen voor dienstreizen met je leidinggevende. Als deze bezoeken naar het oordeel van je leidinggevende voor jouw functie noodzakelijk zijn en in het belang van het Autonoom Gemeentebedrijf, beschouw je deze bezoeken als werk. Indien er geen schijn van corruptie mogelijk is, bewaar dan een evenwicht tussen wat we zelf betalen aan contacten en wat een leverancier of klant betaalt. Zo ontstaat er geen voordeel voor enige partij.

Soms kunnen uitnodigingen voor dienstreizen of bedrijfsbezoeken bedoeld zijn om jou als mogelijke klant of opdrachtgever gunstig te stemmen. Let er samen met je leidinggevende op dat dit je objectiviteit en je oordeelsvermogen niet onbewust beïnvloedt.

4. Behandelen van informatie

Je gaat zorgvuldig om met informatie waarover je beschikt

Je denkt na over welk soort informatie je beschikt. Verspreid die informatie alleen als je zeker bent dat het niet over vertrouwelijke gegevens gaat.

Je mag op vraag van een burger of uit eigen beweging inlichtingen geven over materies waarvoor je bevoegd bent. Maar beleidsplannen die nog niet rijp zijn voor besluitvorming, of informatie over vertrouwelijke dossiers, mag je niet meedelen.

Je hebt de plicht om informatie die betrekking heeft op een individuele cliënt of burger geheim te houden, behalve als de betrokkene zijn uitdrukkelijke toestemming daarvoor gegeven heeft of als daarvoor een andere juridische grond is zoals het gedeeld beroepsgeheim.

Je maakt ook geen feiten bekend die betrekking hebben op:

- de veiligheid van het land
- de bescherming van de openbare orde
- de financiële belangen van de overheid
- het voorkomen en bestraffen van strafbare feiten
- het medische geheim
- het vertrouwelijk karakter van commerciële, intellectuele en industriële gegevens
- het vertrouwelijk karakter van de beraadslagingen

Je maakt geen misbruik van informatie waarover je vanuit je functie beschikt; niet voor jezelf en ook niet voor anderen.

Je houdt geen relevante informatie achter

Je houdt geen relevante informatie (bewust) achter of manipuleert die informatie niet.

De eindgebruiker heeft recht op goede en juiste informatie over alles wat er gedaan of beslist wordt. Ook om de onderliggende argumenten en afwegingen te kennen. Want het handelen van onze organisaties heeft grote invloed op de eindgebruikers.

Daarom zijn we verplicht om te zorgen dat de eindgebruiker nauwkeurig en op tijd op de hoogte is. De communicatiedienst kan je hierbij helpen.

Voor contacten met de pers zijn er wel specifieke afspraken. Wil je informatie verspreiden via de pers, doe het dan in samenspraak met de communicatiedienst en met de (woordvoerders van de) functioneel bevoegde schepen.

Als een journalist jou rechtstreeks aanspreekt, hou je dan aan deze afspraken:

- gaat het om een beleidsmatige vraag: geef niet onmiddellijk antwoord, maar overleg eerst met de communicatiedienst. Zij beoordelen dan of zij en/of de (woordvoerder van de) functioneel bevoegde schepen de journalist te woord zullen staan.
- gaat het om een technische vraag: dan mag je de journalist wel meteen antwoorden. Meld het vervolgens aan je leidinggevende en aan de communicatiedienst, die het op hun beurt aan de functioneel bevoegde schepen doorgeven.

Je verzekert een discrete behandeling van persoonsgegevens

Wanneer je toegang krijgt tot persoonsgegevens, is het heel belangrijk om het vertrouwelijke karakter van die persoonsgegevens te bewaren.

Persoonsgegevens zijn alle gegevens die toelaten iemand direct of indirect te identificeren. Dat kan direct zijn zoals via een naam of rijksregisternummer. Ook een combinatie van schijnbaar onschuldige gegevens laten vaak toe de link te leggen met een specifieke persoon. Wanneer je gegevens verwerkt over een persoon waarvan je het adres in

combinatie met de leeftijd en het geslacht kent, dan spreken we dus ook over persoonsgegevens.

Je zorgt ervoor dat anderen deze gegevens niet kunnen inkijken, aanpassen of verwijderen. Dat doe je bijvoorbeeld door de vertrouwelijke informatie op te bergen of je computer steeds te vergrendelen als je je werkplek verlaat. Wees ook voorzichtig met bijvoorbeeld usb-sticks waarop persoonsgegevens staan.

Op het gebruik van persoonsgegevens en hun verwerking staan er een hele reeks beperkingen. Persoonsgegevens mogen dus niet zomaar voor gelijk wat gebruikt worden. Je geeft standaard dan ook geen persoonsgegevens door aan collega's, behalve als ze dezelfde persoonsgegevens voor hetzelfde doel gebruiken.

Persoonsgegevens doorgeven aan collega's die de gegevens voor andere doeleinden willen gebruiken, mag dus niet. Je mag de vertrouwelijke informatie wel bekendmaken of delen als de betrokkene zijn uitdrukkelijke toestemming daarvoor gegeven heeft of als daarvoor een andere wettelijke grond is.

Je meldt tussenkomsten van mandatarissen

Meld het aan je leidinggevende als een mandataris tussenkomt in een dossier. Daarmee bedoelen we tussenkomsten die verder gaan dan een louter informatieve vraag, of een vraag in het kader van de functionele relatie tussen mandataris en medewerker.

Het gaat zowel om mandatarissen zelf (raadsleden, schepenen, burgemeester, voorzitter…) als om personen die in hun naam spreken (zoals kabinetsmedewerkers).

In elk dossier dat je behandelt moet duidelijk zijn wie advies heeft verleend en wie welke beslissing heeft genomen. Zo bescherm je ook jezelf als er later (kritische) vragen zouden komen over de uitkomst in een dossier. Effectieve tussenkomsten van mandatarissen neem je op in je dossier.

Tussenkomsten van een mandataris om bijvoorbeeld een administratieve procedure in één welbepaald dossier te bespoedigen of inhoudelijk bij te sturen, zijn niet toegelaten. Dit brengt een ongelijke behandeling van klanten of burgers met zich mee.

Wat wel mag, zijn:

- louter informatieve vragen van algemene of technische aard;
- vragen en/of tussenkomsten van mandatarissen in het kader van hun functionele relatie ten aanzien van de medewerkers en diensten.
- Dat soort vragen hoef je uiteraard niet in het dossier op te nemen.

5. Gebruik van bedrijfsmiddelen

Je gebruikt de middelen van het Autonoom Gemeentebedrijf enkel voor je werk

Je draagt zorg voor de bedrijfsmiddelen en gebruikt ze enkel voor je werk. Beperkt en occasioneel privé-gebruik kan in sommige gevallen, maar enkel als dat onze geloofwaardigheid en betrouwbaarheid tegenover de eindgebruiker en burger niet schaadt.

De bedrijfsmiddelen zijn en blijven eigendom van het Autonoom Gemeentebedrijf. Je draagt er zorg voor en je mag ze niet meenemen naar huis. Enkel je leidinggevende kan hiertoe uitdrukkelijk de toestemming geven omwille van functionele of werkgerelateerde redenen. Heb je een laptop, tablet of smartphone dan is het wel toegelaten om deze mee te nemen naar huis, bijvoorbeeld om te telewerken.

Bedrijfsmiddelen omvatten alles wat eigendom is van het Autonoom Gemeentebedrijf of betaald wordt door het Autonoom Gemeentebedrijf, zoals:

- pc's en laptops;
- software
- randapparatuur;
- servers;
- telefoons;
- internettoegang;
- toegang tot sociale media;
- kantoorbenodigdheden;
- werkmateriaal;
- gereedschappen;
- voertuigen;
- werkkleding;
- machines;
- verzorgingsmateriaal;
- …

Privégebruik van bedrijfsmiddelen is bij een overheid een extra probleem omdat je dan publieke middelen gebruikt voor jezelf. Je riskeert je geloofwaardigheid en betrouwbaarheid te verliezen als je bedrijfsmiddelen misbruikt of verspilt. Een voorbeeld: als jij een camionette van je werk gebruikt voor een privé-verhuis, is dat niet eerlijk tegenover je buren die op eigen kosten een camionette moeten huren voor hun verhuis.

Een beperkt en occasioneel privégebruik is soms wel aanvaardbaar. Het is bijvoorbeeld toegelaten om je smartphone of tablet ook privé te gebruiken. Doe dit dan wel buiten de

werkuren (bijvoorbeeld tijdens pauzes of na je uren), en zorg ervoor dat je de productiviteit van de dienst niet hindert.

Het is daarentegen niet toegelaten om je laptop privé te gebruiken, die dient enkel voor je werk. Meer informatie over het gebruik van ICT-materiaal kan je terugvinden in het ICT-afsprakenkader.

Misbruik, dat wil zeggen overmatig, onnodig, storend of schadelijk privégebruik, is uiteraard nooit aanvaardbaar. Denk bijvoorbeeld aan een hele film downloaden, of langdurige privégesprekken voeren met je werktelefoon tijdens je diensturen.

Er bestaat helaas geen duidelijke grens van wat aanvaardbaar is en wat niet. Doe daarom een beroep op je gezond verstand. Als je bedrijfsmiddelen voor privédoeleinden wilt gebruiken, vraag je dan af of je hiervoor goede redenen hebt. Past privégebruik bij een geloofwaardige, zorgvuldige en verantwoordelijke manier van werken? Bij twijfel bespreek je het best eerst met je leidinggevende.

Onkosten moet je bewijzen

Je vraagt enkel een onkostenvergoeding voor werkelijk gemaakte kosten die redelijk en noodzakelijk zijn.

Uitzonderlijk gebeurt het dat je, in overleg met je leidinggevende, zelf kosten maakt bij de uitoefening van je functie. Die kosten kunnen achteraf terugbetaald worden als ze noodzakelijk zijn voor de uitoefening van je functie of nodig voor de dienst.

Je moet de kosten uiteraard kunnen bewijzen, aan de hand een factuur of een kasticket. Enkel kosten die je effectief hebt gemaakt, komen in aanmerking. Daarom zijn bijvoorbeeld een offerte of een kopie van een prijslijst niet voldoende als bewijs.

Het spreekt vanzelf dat je alleen een terugbetaling vraagt van de onkosten die je niet op een andere manier vergoed krijgt. Ook onverantwoord gemaakte of buitensporige kosten worden niet terugbetaald.

6. Gedrag in de privésfeer

Je meldt privérelaties met een integriteitsrisico aan je leidinggevende

Familierelaties, vriendschapsrelaties of liefdesrelaties met collega's of klanten zijn in principe geen probleem. Als er toch een integriteitsrisico aan verbonden is, meld je de relatie aan je leidinggevende en bekijk je samen hoe je dat risico aanpakt.

Overal waar mensen samen komen, kunnen privérelaties ontstaan, dus ook op het werk. Daar is op zich niets mis mee.

In sommige gevallen kan het wel een probleem worden. Er kan (een schijn van) belangenvermenging zijn, er kan een probleem zijn met het delen van vertrouwelijke informatie, of er kunnen nog andere integriteitsrisico's ontstaan.

Anderen kunnen de indruk krijgen dat je een vriend, familielid of lief bevoordeelt in je werk. Het is ook moeilijk om het werk te beoordelen, controleren of goedkeuren van een collega waarmee je een privérelatie hebt.

Een relatie kan bovendien de werkverhoudingen verstoren. Soms tijdens de relatie zelf, soms nadat de relatie is afgebroken. Dat risico is groter bij een machtsverschil, zoals bij een relatie tussen een leidinggevende en een van zijn medewerkers.

Je meldt privérelaties die een risico op een integriteitsschending kunnen vormen, altijd bij je leidinggevende. Afhankelijk van de situatie, maak je dan nieuwe werkafspraken of worden taken anders verdeeld. Soms kan een overplaatsing naar een ander team of een andere dienst een oplossing zijn.

Je doet geen uitspraken die je eigen functioneren of het Autonoom Gemeentebedrijf kunnen schaden

Je mag in je privé-tijd vrij je mening geven. Maar let op dat je ook privé geen uitspraken doet die je eigen functioneren of het Autonoom Gemeentebedrijf kunnen schaden. Als je het niet eens bent met bepaalde beslissingen, bespreek je dat met je leidinggevende in plaats van het openbaar bekend te maken.

Voor iedereen geldt het grondrecht van vrije meningsuiting, dus ook voor ambtenaren. Maar let op: anderen kunnen zelfs jouw privé-uitlatingen zien als uitlatingen van het bestuur, terwijl je helemaal geen bestuurder bent! Doordat je voor het Autonoom Gemeentebedrijf werkt, ben je een ambassadeur van je organisatie, en de buitenwereld ziet jou zo ook.

Gebruik steeds je verstand als je persoonlijke opvattingen wil uiten. Je moet wel extra voorzichtig zijn bij onderwerpen die in het nieuws zijn, of waarvoor belangengroepen en politieke partijen veel aandacht hebben.

Denk extra goed na voor je iets op sociale media zet. De gevolgen kunnen groter zijn dan je verwacht. Kleine dingen, zoals een grappig bedoelde opmerking of afbeelding op Twitter, Instagram, Facebook of andere sociale media kunnen een eigen leven gaan leiden en je werk ineens in een verkeerd daglicht stellen. Besef dat alles op internet gekopieerd en doorgestuurd kan worden naar anderen.

Als je het niet eens bent met bepaalde beslissingen, maak dan je ongenoegen niet in het openbaar bekend. Bespreek dan met je leidinggevende hoe je hiermee om kan gaan.

Luik III. ICT-gedragsregels

7. Veilig gebruik van ICT-middelen

Je gaat zorgvuldig om met je ICT-middelen en beveiligt ze

ICT-veiligheid is een taak van elke medewerker. Je gebruikt je ICT-middelen met zorg en beveiligt zowel de toestellen, de toepassingen als de bijhorende data. Je respecteert het informatieveiligheidsbeleid, de afgeleide regels en de wettelijke bepalingen. Het ICT-veiligheidsbeleid van het Autonoom Gemeentebedrijf en haar partners vind je op Mia.

Je bent aansprakelijk voor alles wat je doet met je persoonlijke gebruikersidentificatie. Deel daarom nooit jouw gebruikersnaam en bijbehorend wachtwoord of pincodes, tokens,… Zo voorkomt je onrechtmatig gebruik. Je respecteert altijd het wachtwoordbeleid.

Je krijgt enkel toegang tot data en applicaties via de geldende procedures. Je krijgt die toegang enkel om je werk te kunnen uitvoeren, met respect voor de deontologische waarden en conform de relevante wetgeving.

Je mag de beveiliging van ICT-middelen niet uittesten of in opspraak brengen, tenzij het tot jouw opdracht behoort en je hiervoor vooraf toestemming kreeg van je leidinggevende.

Je laat je ICT-middelen nooit onbeheerd achter

Je vermijdt dat collega's of bezoekers toegang krijgen tot je persoonlijke gegevens of vertrouwelijke informatie van het Autonoom Gemeentebedrijf en haar partners.

Je laat je ICT-middelen nooit onbeheerd achter en vergrendelt ze telkens als je ze niet gebruikt. Je vermijdt dat afgedrukte documenten rondslingeren op het werk of bij thuiswerken.

Je beschermt jouw ICT-middelen ook tegen diefstal. Je laat ze niet onbeheerd achter op vrij toegankelijke plaatsen of zichtbaar in jouw auto.

Je beschermt je ICT-middelen tegen negatieve invloeden van buitenaf

Je let erop dat je altijd veilige software gebruikt. Je gebruikt geen (illegale) software waarvan je niet zeker bent of je over de juiste licenties beschikt en of ze de beveiliging en performantie van de ICT-infrastructuur in het gedrang kan brengen.

Je gebruikt je ICT-middelen enkel in een vertrouwde omgeving. Je vermijd verbindingen met ongekende of onbeveiligde wifi-netwerken en je gebruikt enkel vertrouwde toestellen om je werk uit te voeren.

Je bent voorzichtig met internet en e-mail. Je denkt twee keer na vooraleer je een link aanklikt of een bijlage opent. Je let op waar je jouw gebruikersnaam, wachtwoord of andere vertrouwelijke informatie ingeeft of achterlaat.

Je meldt veiligheidsincidenten onmiddellijk aan de servicedesk

Je meldt veiligheidsincidenten (bvb. vermoeden van misbruik, verdachte e-mail, eigenaardig gedrag) en verlies of diefstal van ICT-middelen onmiddellijk aan de helpdesk en informeert jouw leidinggevende. Je past de nodige discretie toe over de gemelde incidenten.

8. Goed beheer van ICT-middelen

Je wijzigt zelf niets aan de standaardinstellingen van je ICT-middelen

Het Autonoom Gemeentebedrijf District09 voorziet de ICT-middelen die ze beheert van een standaardconfiguratie. Wijzingen aan hardware, besturingssysteem, configuratie en naamgeving verlopen altijd via de Servicedesk. Je staat wel zelf in voor de licenties en het regelmatig updaten van software die je zelf installeert.

Je gaat zorgvuldig om met eigen ICT-middelen die je voor het werk gebruikt

Gebruik je eigen ICT-middelen die niet door het Autonoom Gemeentebedrijf worden beheerd? Dan kunnen die enkel gekoppeld worden met het bedrijfsnetwerk als ze voldoende beveiligd zijn en als ze vooraf geregistreerd zijn via de helpdesk.

Eigen ICT-middelen die je gebruikt voor het Autonoom Gemeentebedrijf of haar partners, beheer je zoals een goede huisvader. Daarbij sta je in voor:

- de goede zorg en het onderhoud van jouw toestel, zodat je probleemloos je werk kan uitvoeren. Je installeert de nodige updates en voorziet de nodige software om vlot te kunnen samenwerken;
- een degelijk en continu bijgewerkt antivirusprogramma;
- het bewaren van data op de centrale infrastructuur. Je vermijdt lokale opslag van data op jouw ICT-toestellen. Als je toch data opslaat op lokale opslagmedia, dan encrypteer je deze in de mate van het mogelijke.

Wanneer je jouw ICT-middelen niet meer gebruikt voor het Autonoom Gemeentebedrijf of haar partners, dan draag je minimaal de informatie die betrekking heeft op het Autonoom Gemeentebedrijf over en verwijder je die informatie nadien op je persoonlijke opslaglocaties.

9. Gebruik van mobiele opslagmedia en cloud

Je gebruikt maximaal de centrale infrastructuur om data op te slaan

Je verwerkt data maximaal op de centrale infrastructuur of op een door het Autonoom Gemeentebedrijf beheerde locatie. Je mag data enkel buiten de ICT-middelen van het Autonoom Gemeentebedrijf verwerken als je voldoende maatregelen neemt om de data te beschermen.

Je gebruikt enkel occasioneel mobiele opslagmedia voor tijdelijke data

Je mag geen mobiele opslagmedia gebruiken om permanent data op te slaan. Je mag wel occasioneel mobiele opslagmedia (bvb.. USB sticks, externe harde schijven of SD cards) gebruiken. Je slaat de data dan het beste geëncrypteerd op.

Je gebruik geen mobiele opslagmedia van schijnbaar onbetrouwbare partijen.

10. Gebruik van internet

Je gebruikt internet in de eerste plaats voor je werk

De toegang tot internet is in de eerste plaats bedoeld om je werk te kunnen uitvoeren. Je mag internet occasioneel gebruiken voor privédoeleinden, op voorwaarde dat dit gebruik redelijk is, het in geen enkel opzicht de goede werking van het Autonoom Gemeentebedrijf belemmert en geen inbreuk vormt op deze deontologische code.

Je mag geen seksistische, pornografische, racistische of andere extreme sites bezoeken.

Je mag geen gegevens downloaden of verspreiden die beschermd zijn door het recht op intellectuele eigendom, die de toepasselijke wetten schenden of die afkomstig zijn van onbetrouwbare bronnen (zoals spelletjes, films, enz.). Je mag evenmin gebruik maken van websites die spelletjes/games of gokspelen aanbieden.

Als je streaming media bekijkt of beluistert, dan mag dat geen negatieve invloed hebben op je werk of op de performantie van de ICT-infrastructuur.

Regels rond het gebruik van sociale media (Twitter, Facebook, Instagram, internet fora e.d.) zijn bepaald in het standpunt van HR rond sociale media.

11. Gebruik van e-mail

Je gebruikt e-mail in de eerste plaats voor je werk

Het gebruik van e-mail is in de eerste plaats bedoeld om je werk te kunnen uitvoeren. Je mag e-mail occasioneel gebruiken voor privédoeleinden, op voorwaarde dat dit gebruik redelijk is, dit in geen enkel opzicht de goede werking van het Autonoom Gemeentebedrijf belemmert en geen inbreuk vormt op de deontologische code.

Je mag geen persoonlijke financiële verplichtingen aangaan of persoonlijke voorwerpen te koop aanbieden vanuit jouw professionele mailbox.

Je mag niet deelnemen aan kettingbrieven, spamming of discussiefora, tenzij voor je werk.

Je mag geen e-mails versturen waarbij je tracht jouw identiteit te verbergen of te vervalsen.

Je mag geen e-mails versturen of bewaren met onrechtmatige en/of ongepaste inhoud (bvb. obsceen, beledigend, discriminerend, racistisch, politiek, pornografisch, seksistisch, enz.), tenzij je deze kreeg in het kader van de behandeling van een dossier.

Je bent aansprakelijk voor de inhoud van jouw e-mails. Wees je er dus van bewust dat je de toegang tot jouw e-mail altijd afschermt.

12. Privégebruik van ICT-middelen

Je gebruikt de ICT-middelen van het Autonoom Gemeentebedrijf in de eerste plaats voor je werk

Beperkt en occasioneel privégebruik van ICT-middelen kan, maar enkel als het gebruik redelijk is en niet storend voor de werking, en als de performantie en de veiligheid van het netwerk en de infrastructuur niet in het gedrang komen.

Voor bepaalde ICT-middelen zoals een tablet of smartphone is privégebruik toegestaan. Maar ook dan moet je je houden aan de beveiligings- en controlemaatregelen en aan deze deontologische code. Het is daarentegen niet toegelaten om je laptop privé te gebruiken, die dient enkel voor je werk.

Bij een ernstig vermoeden van misbruik, fraude of schending van de richtlijnen, kan het Autonoom Gemeentebedrijf het privégebruik beperken en/of de keuze voor telewerk ontzeggen en desgevallend de vergoeding terugvorderen.

Bewaar geen privébestanden op ICT-materiaal en de netwerkschijven van het Autonoom Gemeentebedrijf.

13. Regels voor beheerders

Onderstaande ICT-gedragsregels zijn enkel van toepassing voor beheerders. Dit zijn medewerkers met verhoogde rechten of administratorrechten. Medewerkers met lokale beheerdersrechten op hun eigen PC of laptop worden hier niet beschouwd als beheerder.

Als beheerder handel je met extra aandacht voor integriteit

Enkel geautoriseerde interne of externe medewerkers kunnen beheerdersrechten krijgen.

Je kan enkel beheerdersrechten krijgen als je deel uitmaakt van de functiegroep die verantwoordelijk is voor het beheer en onderhoud van systemen, netwerk, databases en applicaties.

De beheerdersrechten worden beperkt tot de rechten die noodzakelijk zijn voor het uitvoeren van het toegewezen takenpakket.

Als beheerder mag je nooit taken uitvoeren onder service- of systeemaccounts. Je mag ook de rechten van je eigen gebruikersaccount niet opwaarderen tot beheerdersrechten.

Je mag geen vertrouwelijke of persoonsgegevens raadplegen of verspreiden als dit niet noodzakelijk is binnen je taken van beheerder.

Als beheerder heb je een brede en diepe kennis van je vakgebied en onderhoud je je kennis via opleidingen, certificaten en andere.

Om je integriteit als beheerder te bewaken, worden alle activiteiten van beheerders gelogd.

Je gaat zorgvuldig om met je taken als beheerder

Je voert enkel beheerderstaken uit als gevolg van een geautoriseerde activiteit op basis van een ticket in de ITSM-tool of in het kader van een project. Een uitzondering hierop is het oplossen van incidenten over de veiligheid van het netwerk, systemen of applicaties, de bijbehorende data en de bescherming van de privacy. In zo'n geval zullen de uitgevoerde activiteiten geregistreerd worden in een logboek. Het logboek dient als informatiebron voor de evaluatie van de afhandeling van het incident.

Als beheerder implementeer je de regels die van kracht zijn en volg je deze op.

Interventies op het ICT-materiaal van eindgebruikers kondig je altijd aan en kunnen worden geweigerd door de eindgebruiker.

Bij het aanmaken, aanpassen of verwijderen van een account moet je als beheerder rekening houden met geldende procedures, naamconventie en andere afspraken rond het beheren van accounts.

Als beheerder kijk je regelmatig de logging en monitoring activiteiten na om de operationele werking te garanderen.

De toegekende beheerdersrechten mag je enkel gebruiken voor taken die niet met gewone gebruikersrechten kunnen worden uitgevoerd.

Je bent alert voor het beschermen van informatie

Als beheerders respecteer je de geldende privacywetgeving. Meer informatie over de privacywetgeving is terug te vinden op Mia. Bij vermoeden van inbreuk op de wetgeving, rapporteer je dat direct aan de functionaris voor gegevensbescherming.

Je neemt technische en organisatorische maatregelen om de vertrouwelijkheid van de informatie waarmee je in aanraking komt te waarborgen.

Veranderingen aan configuraties kunnen risico's met zich meebrengen. Als beheerder moet je hier bewust mee omgaan.

Bij vermoeden van ongeautoriseerde handelingen op systemen of applicaties moet je dit als beheerder onmiddellijk rapporteren aan de helpdesk en moet je jouw leidinggevende informeren.

Luik IV: Naleven deontologische code

14. Toepassen van de gedragsregels

Twijfels over de juiste toepassing van de gedragsregels bespreek je met je leidinggevende

Je leidinggevende is je eerste aanspreekpunt als je twijfels hebt over de juiste toepassing van de gedragsregels uit de deontologische code.

De 'gedragsregels' in de deontologische code kunnen niet op alle situaties een kant-en-klaar antwoord bieden. Ze helpen je wel bij al je handelingen en beslissingen, en beschermen je tegen vergissingen of misstappen door onwetendheid.

Toch zal het soms gebeuren dat je twijfelt. Spreek je leidinggevende over je twijfels aan. Kan je niet bij je eigen leidinggevende terecht, richt je dan tot zijn leidinggevende of de algemeen directeur van het Autonoom Gemeentebedrijf.

Het is belangrijk om met elkaar te praten over risico's en morele dilemma's. Zo kan je leren van elkaar. Twijfels met elkaar bespreken voorkomt vaak integriteitsschendingen en kan je helpen bij hoe je moet omgaan met lastige situaties.

Je kan bijvoorbeeld ook aan je leidinggevende vragen om op jullie teamoverleg de concrete toepassing van een bepaalde gedragsregel te agenderen.

Je meldt (vermoedens van) integriteitsschendingen

Als je bij de uitoefening van je werk inbreuken tegen de deontologische code vaststelt, kan je dit melden.

Als je een vermoeden van een integriteitsschending hebt, meld je dit aan je leidinggevende. Ook hier geldt: als je niet bij je eigen leidinggevende terecht kan, richt je dan tot zijn leidinggevende of de algemeen directeur van het Autonoom Gemeentebedrijf.

In overleg met de bevoegde diensten kan beslist worden hiertegen op te treden.

15. Individuele controle

Recht op controle

Het Autonoom Gemeentebedrijf kan je ICT-werkmiddelen controleren, maar enkel binnen het wettelijk kader en mits het respecteren van het recht op je privéleven.

Zo kan het Autonoom Gemeentebedrijf controles doen van:

- het e-mail gebruik
- het internet gebruik
- het gebruik van andere professionele elektronische communicatiemiddelen zoals Spark, Slack, Skype, Teams…
- de informatie en bestanden die medewerkers publiceren op het intranet of internet;
- de informatie en bestanden die medewerkers raadplegen of opslaan op verschillende opslagmedia (mappen op computers, servers, document management systemen, enzovoort).

Doel van de controles

Het Autonoom Gemeentebedrijf kan je ICT-werkmiddelen alleen controleren met het oog op één van de vijf volgende doelen:

1. **Voorkomen en vaststellen van ongeoorloofde feiten, lasterlijke feiten of feiten die strijdig zijn met de goede zeden of die de waardigheid van een andere persoon kunnen schaden.** Dat zijn feiten zoals:
    - het kraken van computers en op een illegale manier kennis nemen van persoonsgegevens of vertrouwelijke medische bestanden;
    - het raadplegen van sites die
        - zich tegen de grondbeginselen van de democratie en de rechtsstaat keren, zoals sites die verband houden met racisme, terrorisme of discriminatie;
        - anderen kunnen kwetsen of beledigen, zoals sites met racistische of seksistische onderwerpen, pornografisch materiaal of schokkende foto's;
        - een gevaar voor verslaving vormen zoals goksites en pornografische sites;
        - het privéleven van iemand aantasten.
2. **Beschermen van informatie die niet geschikt is om algemeen te delen** en die de belangen van het Autonoom Gemeentebedrijf mogelijks kunnen schaden.
3. **Verzekeren van de veiligheid, de performantie of de goede technische werking van de IT-systemen** van het Autonoom Gemeentebedrijf. Daar hoort de controle op de bijhorende kosten en de fysieke bescherming van de ICT-omgevingen en -installaties van het Autonoom Gemeentebedrijf bij.
4. **Te goeder trouw naleven van deze deontologische code.**
5. **Verzekeren van de continuïteit van de dienstverlening** bij overlijden, onvoorziene afwezigheid of vertrek van een werknemer.

De gegevens die verzameld en verwerkt worden voor een controle met het oog op een van de vijf bovenstaande doelen, kunnen niet gebruikt worden voor een controle met andere doeleinden. Als een wettelijke bepaling dat toestaat of oplegt, kan het Autonoom Gemeentebedrijf de gegevens voor een ander doel gebruiken, inkijken en herleiden tot de bepaalde gebruiker.

Soorten controle

De manier waarop het Autonoom Gemeentebedrijf controleert, is afhankelijk van het doel van de controle. Er zijn drie soorten controles:

1. Permanente globale controle

Dit is het automatisch monitoren of bewaren van elektronische communicatiegegevens. Het gaat om niet-geïndividualiseerde gegevens die niet gelinkt (kunnen) worden aan een persoon.

2. Occasionele globale controle

Bij een occasionele globale controle gaat het Autonoom Gemeentebedrijf globale online communicatiegegevens van een bepaalde groep gebruikers over een beperkte periode verzamelen en bekijken. Het Autonoom Gemeentebedrijf kan voor de eerste vier doelen een occasionele globale controle doen.

Een occasionele globale controle kan niet slaan op gegevens uit het verleden en is beperkt tot de tijd die nodig is om eventuele misbruiken te voorkomen of vast te stellen.

3. Individuele controle

Het voorwerp van de individuele controle van ICT-middelen, de doelen en voorwaarden van deze soort van controle zijn in lijn met de aanbeveling van de Gegevensbeschermingsautoriteit van 2/05/2012.

Voorwerp van de controle

Bij een individuele controle, controleert het Autonoom Gemeentebedrijf:

- wie, welke websites heeft bezocht, wanneer en voor hoe lang;
- wie bepaalde e-mails heeft verzonden, de geadresseerden en het volume ervan. Het Autonoom Gemeentebedrijf kan ook de verzonden werkgerelateerde e-mails lezen omdat het haar medewerkers aanbeveelt persoonlijke e-mails te verzenden via een privé-account (Hotmail, Gmail, …).

Wanneer is een individuele controle toegestaan?

Als	Bijkomende randvoorwaarden
Uit een occasionele globale controle blijkt dat de medewerker de ICT-middelen niet heeft gebruikt volgens de afspraken van deze ICT-gedragsregels of andere richtlijnen voor het gebruiken van online technologieën.	De individuele controle kan in deze situatie alleen nadat het Autonoom Gemeentebedrijf: • de betrokken medewerker op een duidelijke en begrijpelijke manier heeft ingelicht over het bestaan van de onregelmatigheid;

	• de medewerkers op de hoogte heeft gebracht dat de elektronische online communicatiegegevens geïndividualiseerd zullen worden als opnieuw een dergelijke onregelmatigheid wordt vastgesteld (= directe individualisering).
Uit een occasionele globale controle blijkt dat een medewerker zich schuldig maakt aan: • ongeoorloofde feiten, lasterlijke feiten of feiten die strijdig zijn met de goede zeden of die de waardigheid van een andere persoon kunnen schaden; • het openbaar maken van vertrouwelijke informatie • feiten die de veiligheid, de performantie of de goede technische werking van de IT-systemen van het Autonoom Gemeentebedrijf in het gedrang brengen.	In die gevallen moet de betrokken gebruiker **niet vooraf worden gewaarschuwd** (= directe individualisering).
Het Autonoom Gemeentebedrijf een **gegrond vermoeden** heeft dat een medewerker zich schuldig maakt aan de feiten, vermeld in het vorige punt. In dat geval, kan het Autonoom Gemeentebedrijf het internetgebruik en e-mailverkeer van de medewerker laten controleren. Het Autonoom Gemeentebedrijf kan dat zonder zich te beroepen op gegevens die verzameld zijn in een eerder uitgevoerde occasionele globale controle. Met 'gegrond vermoeden' wordt bedoeld dat er nog andere **feitelijke elementen** (bijvoorbeeld pestmails) zijn die erop wijzen dat een bepaalde medewerker zich schuldig zou maken aan de feiten vermeld in het vorige punt. De verantwoordelijkheid dat er een gegrond vermoeden is, ligt bij de leidinggevende. Zij moeten in voorkomend geval voor de rechter kunnen bewijzen dat er zo'n gegrond vermoeden was.	Deze controle is **beperkt in de tijd en kan niet slaan op gegevens die in het verleden zijn ontstaan**. De betrokken medewerker hoeft niet op voorhand gewaarschuwd te worden (= directe individualisering).
Een medewerker overleden of onvoorzien afwezig is of de dienst heeft verlaten en niet bereikt kan	Het Autonoom Gemeentebedrijf laat toe om persoonlijke e-mails te versturen met het

worden. In dat geval kan het Autonoom Gemeentebedrijf het werkgerelateerde e-mailverkeer en de werkgerelateerde bestanden op de opslagmedia van de betrokken medewerker raadplegen. Het doel daarvan is de continuïteit van de dienstverlening te garanderen.	professioneel e-mailadres, maar raad aan deze e-mails te bewaren in een map “Privé” binnen de mailbox. Daarom kan het e-mailaccount en de opslagmedia van de afwezige medewerker ook persoonlijke – niet-werkgerelateerde – berichten en informatie bevatten. Dan gebeurt het raadplegen via de functionaris voor gegevensbescherming of een medewerker belast met integriteitszorg. Die kan dan nagaan welke berichten en informatie werkgerelateerd zijn en dus mogen worden ingezien door de leidinggevende en welke persoonlijk zijn.
De wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk wordt geschonden. De wet verplicht de werkgever tot een **onderzoek bij feiten van geweld, pesterijen en ongewenst seksueel gedrag**. Het lijnmanagement is daarbij bevoegd om de verzamelde elektronische online communicatiegegevens te individualiseren.	Het gaat daarbij zowel om de gegevens die werden verzameld bij een occasionele controle als de gegevens die werden verzameld bij de permanente controle. Met dat doel kunnen ook gegevens die in het verleden zijn ontstaan, worden geraadpleegd.
Er **ernstige indicaties** zijn van mogelijke **onregelmatigheden**. In dat geval kan **Audit Vlaanderen** een forensische audit (administratief onderzoek) instellen naar de aangelegenheid in kwestie. De bevoegdheid van Audit Vlaanderen op dat vlak is expliciet opgenomen in artikel 34 van het kaderdecreet bestuurlijk beleid van 18 juli 2003. Datzelfde artikel bepaalt ook dat Audit Vlaanderen voor het uitoefenen van zijn bevoegdheden toegang heeft tot alle informatie. Audit Vlaanderen is in het kader van de uitvoering van zijn forensische audits ook bevoegd om **alle werkgerelateerde e-mailverkeer, werkgerelateerde bestanden en elektronische communicatiegegevens te onderzoeken**.	Die onderzoeksmogelijkheid wordt niet beperkt door het moment waarop de e-mails, bestanden of gegevens zijn ontstaan. De betrokken medewerker hoeft niet vooraf gewaarschuwd te worden (= directe individualisering). Audit Vlaanderen kan dergelijke gegevens eveneens gebruiken in het kader van een detectieaudit, op voorwaarde dat wordt gewaakt over de vertrouwelijkheid van de onderzochte gegevens in de rapportering.
Uit een permanente of occasionele controle blijkt dat een medewerker van de elektronische middelen de **veiligheid, performantie en/of goede technische werking** van de IT-systemen **in het gedrang** brengt of de **kosten abnormaal hoog** doet oplopen	In dat geval kan het Autonoom Gemeentebedrijf nagaan wie de medewerker is met een directe individualisering.

16. Sancties bij niet-naleving

Handel je als interne medewerker niet volgens de deontologische code? Dan kan dit aanleiding geven tot disciplinaire acties zoals vermeld in het arbeidsreglement. Ben je externe medewerker, interim of stagiair? Dan kan je contractuele overeenkomst opgeschort of verbroken worden bij het niet naleven van de deontologische code.

Uitzonderingen op dit beleid zijn enkel mogelijk mits grondige motivatie en een formele goedkeuring van het directiecomité.

Luik V. Definities, referenties en verwijzingen naar regelgeving

Definities

Term	Beschrijving
ICT-middelen	PC's, laptops, servers, smartphones, randapparatuur, netwerk, internet, intranet, e-mail, software, ...
Medewerkers	Interne en externe medewerker, stagiairs en interims
Beheerders	Gebruikers met verhoogde of administratorrechten. Gebruikers met lokale beheerdersrechten op hun eigen PC of laptop worden in deze ICT-code niet beschouwd als beheerder.
Bedrijfsnetwerk	Het bedrijfsnetwerk omvat alle netwerken van District09, met uitzondering van de publieke of bezoekersnetwerken

Referenties

Term	Meer info
ICT-veiligheidsbeleid	Veiligheidsbeleid op mia.gent
Wachtwoordbeleid	Wachtwoordbeleid op mia.gent
Beheerdersaccounts	adm1, adm2 of adm3 accounts
Functionaris voor gegevensbescherming	privacy@District09.gent
Helpdesk	servicedesk@District09.gent
Intranet	https://mia.gent

Regelgeving

Niet-exhaustieve lijst van wetten en reglementeringen over de deontologische code:

- Grondwet
- Strafwetboek
- Wetboek van Strafvordering
- Wet van 29 juli 1991 betreffende de uitdrukkelijke motivering van de bestuurshandelingen
- General Data Protection Regulation (GDPR) – Algemene Verordening Gegevensbescherming (AVG)
- Wet van 11 april 1994 betreffende de openbaarheid van bestuur
- Wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk
- Wet van 14 december 2000 tot vaststelling van sommige aspecten van de organisatie van de arbeidstijd in de openbare sector
- Wet van 10 mei 2007 ter bestrijding van bepaalde vormen van discriminatie
- Wet van 10 mei 2007 ter bestrijding van discriminatie tussen vrouwen en mannen
- Wet van 10 mei 2007 tot aanpassing van het Gerechtelijk Wetboek aan de wetgeving ter bestrijding van discriminatie en tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden
- Gemeente- en OCMW-decreet – Decreet van 22 december 2017 over het lokaal bestuur
- Rechtspositieregeling (RPR) Autonoom Gemeentebedrijf District09

Aanvaarding

Door de ondertekening van deze deontologische code verklaar ik als medewerker of beheerder dat ik kennis heb genomen van de opgenomen regels en engageer ik mij tot het naleven ervan.

Datum

Naam en voornaam

Handtekening