

Gedragscode informatieVeiligheid & Privacybescherming

voor Mandatarissen

DPO

Frank Desmet

Goedgekeurd door gemeente- en OCMW raad van 26 januari 2022

Gedragscode informatieVeiligheid & Privacybescherming

Inhoud

[Toepassingsgebied 2](#_Toc93060633)

[Professioneel werken 2](#_Toc93060634)

[Wachtwoorden 3](#_Toc93060635)

[Clean Desk & Clean Screen 3](#_Toc93060636)

[Hardware/Software 4](#_Toc93060637)

[Data opslag & back-up 4](#_Toc93060638)

[USB-sticks of ander mobiele opslagmedia 5](#_Toc93060639)

[Beveiliging 5](#_Toc93060640)

[Derden 5](#_Toc93060641)

[Privacy van de mandataris 6](#_Toc93060642)

[Controle gemeente en OCMW Beersel 6](#_Toc93060643)

[Meldplicht van inbreuken, risico’s en gegevenslekken 6](#_Toc93060644)

[Sanctie 7](#_Toc93060645)

[Voor akkoord 7](#_Toc93060646)

**In gebruik vanaf:**
27/01/2022

# Toepassingsgebied

Deze gedragscode is van toepassing op alle mandatarissen van de gemeente en het OCMW die in contact komen met of instaan voor de verwerking van persoonsgegevens[[1]](#footnote-1), vertrouwelijke of zeer vertrouwelijke gegevens.

Elke mandataris is persoonlijk verantwoordelijk voor de aan hem toevertrouwde persoons- en andere gegevens krachtens het beroepsgeheim en de discretieplicht. Bijzondere aandacht geldt voor de gegevens uit de Kruispuntbank Sociale Zekerheid (KSZ), het Rijksregister, het Centraal Strafregister en/of andere bronnen met gevoelige persoonsgegevens (bijvoorbeeld GAS boetes).

Deze gedragscode is niet beperkt tot persoonsgegevens, maar is ook toepasbaar op gevoelige en vertrouwelijke bedrijfsinformatie.

Elke mandataris is persoonlijk verantwoordelijk voor het gebruik van het aan hem/haar ter beschikking gestelde materiaal (ongeacht in welke vorm) waarmee hij/zij toegang krijgt tot de gegevens en gebouwen zoals daar zijn laptops, toegangsbadges, sleutels, … enzoverder. Alsook de aan hem/haar toegewezen toegangscodes, gebruikersaccounts, wachtwoorden, … enzoverder.

# Professioneel werken

**De mandataris is professioneel in het gebruik van e-mail, intranet, internet, sociale media, enzoverder.**

* **Gemeente- en OCMW diensten zullen enkel naar het e-mailadres @beersel.be communiceren met de mandatarissen.**

Wat doe je absoluut **niet** via hard- of software van de organisatie? (niet limitatieve lijst)

* Berichten, die als een aantasting van iemands menselijke waardigheid kunnen beschouwd worden, doorsturen. Bijvoorbeeld berichten, die door de ontvanger, ervaren kunnen worden als racistisch, discriminerend (op basis van geslacht, seksuele geaardheid, godsdienst, afkomst, handicap, …), seksueel intimiderend, enzoverder.
* Bestanden met aanstootgevende, pornografische of racistische inhoud consulteren, downloaden, openen of verspreiden. Zelfs niet indien het gaat om wettelijk toegelaten publicaties. De dienst ICT blokkeert op het intern netwerk ongepaste sites zo veel mogelijk.
* Deelnemen aan kettingmails.
* Ontvangen e-mails doorsturen naar een elektronisch adres buiten de organisatie (bijvoorbeeld naar een privé e-mailadres).
* Gegevens in strijd met auteursrechten verspreiden of downloaden.
* Bestaande veiligheidsmaatregelen of richtlijnen niet in acht nemen, omzeilen of neutraliseren, of proberen dit te doen. Bijvoorbeeld ‘verboden’ bestanden hernoemen om deze toch te kunnen raadplegen.
* Zich onrechtmatig toegang verschaffen tot de informaticasystemen van de organisatie.
* Zich onrechtmatig toegang verschaffen tot afgesloten en/of beveiligde ruimtes.
* De goede werking van de informatiesystemen belemmeren of verhinderen.
* Op eender welke manier, ongeautoriseerd, vertrouwelijke persoons-, klant- of bedrijfsgegevens verspreiden.
* De vertrouwelijkheid en integriteit van de gegevens schenden of hun beschikbaarheid belemmeren.
* Foutieve informatie, om de organisatie of medewerkers in een slecht daglicht te plaatsen, bewust doorgeven.
* Bij het beëindigen van de functie wordt de mailbox door **de gemeente/ OCMW Beersel** maximum 30 dagen bewaard. Na 30 dagen wordt de mailbox onherroepelijk verwijderd. Belangrijke mails kunnen gearchiveerd worden. Dit kan gedaan worden door de hulp in te roepen van de dienst ICT.

**Mandatarissen verbinden zich ertoe enkel in opdracht van de organisatie te handelen bij het verwerken van gegevens.**

Je verschaft je enkel toegang tot de gegevens, die noodzakelijk zijn voor het uitvoeren van de aan jou toevertrouwde opdracht(en). Je vertrouwt gegevens, waarvan je kennisneemt, enkel toe aan anderen in de mate dat dit voor de uitvoering van jouw opdracht noodzakelijk is en op voorwaarde dat deze persoon (aan wie je de gegevens kenbaar maakt) gemachtigd is er kennis van te nemen. Elke mandataris is verantwoordelijk voor zijn/haar communicatiegedrag.

Het bewaren van vertrouwelijkheid van gegevens en informatie, waarmee je in aanraking komt, blijft gelden na beëindiging van de opdracht of taken, die je toegewezen werden, ook na het beëindigen van je functie als mandataris. Je bezorgt op het einde van je opdracht (bijvoorbeeld bij einde functie als mandataris) of op het einde van tewerkstelling alle eventuele gegevensdragers of kopieën (papier, digitaal, …) met vertrouwelijke en zeer vertrouwelijke gegevens terug aan de organisatie.

# Wachtwoorden

**Álle wachtwoorden zijn strikt persoonlijk en worden niet gedeeld**. Dit houdt in dat je als mandataris enkel met je eigen gebruikersnaam en wachtwoord mag inloggen.

De sterkte van een wachtwoord is voornamelijk afhankelijk van de lengte ervan. Hoe langer een wachtwoord, hoe sterker. Het gebruik van een mengeling van hoofdletters, kleine letters, cijfers en speciale tekens is verplicht. Meer informatie over hoe je een goed wachtwoord kan kiezen, vind je terug in het wachtwoordbeleid**.**

Wees zeer voorzichtig met het opschrijven of bewaren van je wachtwoorden. Zo vermijd je dat een derde toegang krijgt tot alle informatie (bedrijfsinformatie en/of persoonsgegevens) waar jij toegang tot hebt (bijvoorbeeld via netwerkdrives, jouw e-mails, de door jouw gebruikte applicaties, enzoverder). Dit is extra belangrijk bij gebruik van laptops, tablets/iPads, externe gegevensdragers en andere mobiele toestellen.

Bijvoorbeeld

* Schrijf nooit je wachtwoord op een post-it of sticker, die je plakt op je laptop, tablet/iPad of scherm van een desktop.
* Bewaar je wachtwoorden niet in een bestand dat je “paswoorden.txt” noemt.
* Gebruik geen standaardwachtwoorden, zoals bv. Paswoord123.
* Maak eventuele pincodes voor het ontgrendelen van je GSM niet voor de hand liggend en lang genoeg. Dus geen 1111, 1234, je geboortedatum, enzoverder. Kies liever voor een code die langer is dan de standaard 4 cijfers als dat technisch mogelijk is. In Beersel worden 6 cijfers gebruikt.
* MFA (Multi Factor Authentication) wordt overal gebruikt indien de toepassing het toelaat. Voor het gebruik van M365 is het verplicht.

# Clean Desk & Clean Screen

**Dankzij de toepassing van onderstaande goede praktijken beperk je het risico van ongewettigde toegang of beschadiging van hard- en software.**

Bijvoorbeeld:

* Zet je pc/laptop in sluimerstand als je hem niet gebruikt of wanneer je je plaats verlaat. Zo kan niemand je pc/laptop gebruiken in jouw naam of alle gegevens en applicaties erop raadplegen.
* Het is een goede gewoonte om je computer te vergrendelen (toets + L) wanneer je je plaats verlaat. Op deze manier is je computer beveiligd met je wachtwoord en kan niemand je computer in jouw naam gebruiken.
* Zorg ervoor dat alle gevoelige papieren of elektronische documenten zich achter slot bevinden in de daartoe bestemde kasten bij het verlaten van de werkruimte. Ruim 's avonds voor je vertrekt, je bureau op, sluit je pc/laptop af en berg alle gevoelige informatie en/of dragers (ook papieren) op een veilige plaats, bijvoorbeeld een locker, op.
* Probeer er, in de mate van het mogelijke, voor te zorgen dat documenten met gevoelige informatie niet onbewaakt achtergelaten worden op printer, fax, etc.
* Waak erover dat opslagtools (zoals bijvoorbeeld USB-sticks, sd kaartjes, cd roms, dvd’s, …) niet onbewaakt achtergelaten worden.

# Hardware/Software

**Als je met persoons-, bedrijfs-, vertrouwelijke en gevoelige informatie werkt, wees je dan bewust van een aantal veiligheidsrisico’s die hieraan verbonden zijn:**

Bijvoorbeeld:

* Verlies van vertrouwelijke, gevoelige of persoonsinformatie ten gevolge van diefstal, verlies of schade van het toestel
* (Niet-)intentionele verspreiding van vertrouwelijke, gevoelige of persoonsinformatie
* Kwaadwillige aanvallen zoals malware, ransomware, spyware, virussen, phishing, enz.
* Frauduleuze aanvallen of pogingen om toegang te verkrijgen tot vertrouwelijke, gevoelige of persoonsinformatie
* Continuïteit en beschikbaarheid van de informatiesystemen
* Naleving van de wetgeving betreffende de persoonlijke levenssfeer, informatieveiligheid en gegevensbescherming
* Je mag op je laptop, indien eigendom van de gemeente, voor elke vorm van communicatie uitsluitend gebruik maken van software die door de dienst ICT geïnstalleerd is. Dienst ICT zorgt voor de juiste licenties. Heb je nood aan andere software op je laptop, neem dan contact op met de dienst ICT.
* Op persoonlijke laptops adviseren we om enkel standaardtoepassingen te gebruiken.

Intellectuele eigendomsrechten moeten steeds gerespecteerd worden.

Je transfereert geen software die door de organisatie aan jou ter beschikking wordt gesteld over naar eigen apparatuur, behoudens toestemming van de dienst ICT.

# Data opslag & back-up

**Dienst ICT zorgt voor een automatische back-up van alles wat gebruikt wordt via de netwerkinfrastructuur van de organisatie.**

Dit houdt in:

* Er wordt geen back-up gemaakt van wat in de publieke Cloud (b.v. Dropbox) staat. Voor Microsoft toepassingen M365, zal kunnen terug gegaan worden tot versie -249. Dat is versiebeheer maar wordt niet aanzien als back-up.
* Bij e-mail wordt een retentietijd gegarandeerd tot 90 dagen.
* Dienst ICT kan geen back-up maken van gegevens, die je lokaal bewaart op je mobiele toestel(len).
* Het is dan ook af te raden om persoonsgegevens of vertrouwelijke informatie lokaal op je toestel te bewaren.
* Van je pc of laptop dien je zelf een back-up te maken.
* Het wordt ten zeerste afgeraden gebruik te maken van publiek aangeboden kanalen (bijvoorbeeld de gratis aangeboden versie van Dropbox), onbeveiligde of onvoldoende beveiligde platformen om gevoelige of vertrouwelijke gegevens te bewaren of uit te wisselen.

# USB-sticks of ander mobiele opslagmedia

**Mobiele opslagmedia moeten met de nodige aandacht worden behandeld.**

* Als je bestanden van een USB-stick of ander mobiel opslagmedium op je laptop wil plaatsen, scan dit dan eerst op virussen of andere bedreigingen.
* Als iemand je vraagt om bestanden vanop jouw pc te kopiëren naar zijn of haar pc, gebruik dan je eigen USB-stick. Scan je stick opnieuw met je virusscanner wanneer je deze terugkrijgt en zeker vooraleer je hem terug gebruikt.
* Het is aan te raden geen vertrouwelijke gegevens en/of persoonsgegevens op een USB-stick of andere mobiele gegevensdrager te plaatsen. USB-sticks worden makkelijk vergeten of raken verloren.
* Eén van de tactieken van cybercriminelen is USB-sticks te laten rondslingeren op openbare plaatsen (bv. Café, stations, bedrijfsparking, …). Deze sticks zijn mogelijk besmet met virussen of spionagesoftware. Steek een USB-stick, die je vindt of waarvan je de oorsprong niet kent, dus nooit in je toestel.
* Vind je een vergeten USB-stick na een presentatie in een vergaderzaal, bezorg deze dan aan de dienst ICT of de functionaris voor gegevensbescherming.
* Als je op een publieke computer een presentatie geeft, is het best je presentatie op je USB-stick te laten staan en vandaar op te starten. Als je toch eerst je presentatie naar de andere pc kopieert, vergeet dan zeker niet de presentatie nadien te verwijderen (shift + delete). Anders blijft jouw presentatie voor altijd op de publieke pc (al dan niet in de prullenmand) staan.

# Beveiliging

**Het netwerk van de gemeente/OCMW Beersel is standaard beveiligd.**

* Als je via andere (gratis) aangeboden verbindingen werkt (hotspots, wifi, hotels, ...), is dit niet altijd het geval. Beperk dit tot het absolute minimum. Raadpleeg geen persoonsgegevens of andere gevoelige informatie via een onbeveiligde verbinding of een verbinding waarvan je niet zeker weet dat ze veilig is.
* Beveiligingssoftware (antivirus, antispam, firewall, …) op diensttoestellen schakel je niet uit of wijzig je niet.
* Als je toegang wil op het netwerk of de applicaties van de organisatie (bv om e-mails te lezen) via een ander toestel dan je diensttoestel, kan dit enkel indien er op dit toestel up-to-date beveiligingssoftware geïnstalleerd en geactiveerd is. MFA wordt gebruikt.
* Mobiele toestellen (tablet, smartphone, …) moeten verplicht beveiligd zijn met een voldoende sterke pincode. Hou hierbij in het achterhoofd “hoe meer cijfers hoe veiliger”. Probeer op z’n minst een code met 6 cijfers in te stellen. Je kan het toestel ook beveiligen met een vingerafdruk of dergelijke, maar niet alle toestellen bieden deze mogelijkheid.
* Dienst ICT kan verifiëren of de configuratie en veiligheidssoftware van een toestel conform is. In geval van afwijkingen, brengt de dienst ICT verslag uit aan het informatieveiligheidsteam.

# Derden

**De door de gemeente/OCMW Beersel ter beschikking gestelde diensttoestellen mogen niet gebruikt worden door derden.**

Ook niet indien er geen gebruik wordt gemaakt van een netwerkverbinding, tenzij onder toezicht van een medewerker van de organisatie. Bijvoorbeeld in het kader van een opleiding, presentatie, … voor onze organisatie.

Indien je werkt via een data-abonnement met tussenkomst van de gemeente/OCMW Beersel, mag een derde geen gebruik maken van dit abonnement.

Als je werkt in een omgeving in aanwezigheid van derden, zorg er dan voor dat deze geen toegang hebben tot de informatie of persoonsgegevens toebehorend aan de organisatie. Als je bijvoorbeeld in een druk station je e-mails leest, zorg er dan voor dat niemand over je schouder kan meelezen.

# Privacy van de mandataris

**De organisatie verzamelt, bewaart en verwerkt gegevens van de mandatarissen van de organisatie. Deze gegevens worden opgenomen en bewaard in bestanden, zowel op papier als digitaal, en worden enkel gebruikt in het kader van personeelsadministratie/loonadministratie.**

* De houder van de bestanden is het bevoegd bestuursorgaan, College van Burgemeester & Schepenen of Vast Bureau. De verantwoordelijke voor het dagelijks bestuur is de Algemeen Directeur.
* Elke mandataris heeft het recht om zijn/haar gegevens op te vragen. Dit kan via de personeelsdienst.
* Elke wijziging van je gegevens wordt, zo snel en volledig mogelijk, doorgegeven aan de dienst beleidsondersteuning.
* Als je vragen of bezorgdheden hebt over de verwerking van je gegevens kan je je in eerste plaats wenden tot de functionaris van de gegevensbescherming (DPO) van gemeente / OCMW Beersel via dpo@beersel.be
* In tweede instantie kan je je wenden tot de Vlaamse Toezichtcommissie (VTC). De contactgegevens kan je vinden op hun website [Vlaamse Toezichtcommissie | Vlaanderen Intern](https://overheid.vlaanderen.be/vlaamse-toezichtcommissie)

# Controle gemeente en OCMW Beersel

**Gemeente en OCMW Beersel respecteren de privacy van de mandatarissen. Toch zullen een aantal controlemaatregelen genomen worden, om de goede werking van de apparatuur en naleving van toepasselijk regelgeving te verzekeren. De algemeen directeur, ICT-verantwoordelijke en functionaris voor gegevensbescherming (DPO) waken over de naleving.**

* Bij controles of screening door middel van aangepaste software worden inhoudelijke gegevens in principe niet ingekeken. In de mate zij zouden ingekeken moeten worden, wordt de vertrouwelijkheid door de dienst ICT gegarandeerd.
* De functionaris voor gegevensbescherming (DPO) zal controles uitvoeren op de naleving van toepasselijke wet- en regelgeving, gedragscodes, richtlijnen, afspraken, enzoverder in het kader van informatieveiligheid en gegevensbescherming.
* Bij vermoeden van misbruik of overtredingen wordt de algemeen directeur ingelicht. Zij geeft opdracht om een onderzoek in te stellen. In dat geval kan bijvoorbeeld het e-mail- en internetgebruik van een mandataris nader bekeken worden. De controles zullen beperkt zijn en evenredig met de aard van het vermoede misbruik. Doorgedreven onderzoek, waarbij alle gegevens en inhoud van alle verrichtingen via e-mail en internet onderzocht worden, is enkel mogelijk bij aantoonbare en ernstig vermoeden van misbruik.

# Meldplicht van inbreuken, risico’s en gegevenslekken

**Elke mandataris is verplicht, waar nodig, gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht ervan.**

* Je meldt inbreuken, of bij een vermoeden ervan, zo snel mogelijk aan het informatieveiligheidsteam. Dit kan via e-mail naar dpo@beersel.be
* Je meldt elk (mogelijk) probleem met het netwerk, elk misbruik van de internet- en e-mailfunctionaliteiten (virussen, pogingen tot intrusie of hacking, ...), ongeacht of dit op het niveau van de centrale computers, het netwerk, de lokale computers of de software is, zo snel mogelijk aan ict@beersel.be.. De dienst ICT verwittigt de functionaris voor gegevensbescherming (DPO).
* De mandataris neemt de gepaste geheimhouding in acht ten opzichte van anderen met betrekking tot (vermoedelijke) inbreuken, risico’s en problemen.
* Bij diefstal van een toestel dat informatie, data waarvan gemeente / OCMW Beersel eigenaar is, bevat, doe je aangifte bij de politie en bezorg je een kopie van je aangifte aan de dienst ICT. Samen met jou wordt nagegaan of er effectief sprake is van een inbreuk met betrekking tot persoonsgegevens (gegevenslek). De dienst ICT verwittigt de functionaris voor gegevensbescherming (DPO) die op zijn beurt oordeelt of de Vlaamse Toezicht commissie ingeschakeld moet worden.

# Sanctie

Niet-naleving van deze gedragscode kan beteugeld worden conform de deontologische code voor mandatarissen.

# Voor akkoord

|  |  |
| --- | --- |
| Datum |  |
| Naam + Voornaam |  |
| Handtekening |  |

1. De Algemene Verordening Gegevensbescherming 2016/679 (EU) (AVG/GDPR) van 27 april 2016 en toepasselijke regelgeving(en) inzake privacy en gegevensbescherming zijn van toepassing. [↑](#footnote-ref-1)