

Integriteits- en geheimhoudingsverklaring

Externe Medewerkers

Achternaam en voorletters	
Geboortedatum en -plaats	
Functie	
Naam van eenheid/dienst	

Verklaart het volgende:

1. Geheimhouding

Ik verklaar geheim te houden alle informatie die mij gedurende mijn werkzame periode ter kennis komt waarvan ik weet of vermoed dat deze vertrouwelijk is.

Persoonsgegevens, financiële gegevens, klantgegevens, aanbestedingsgegevens en contractgegevens beschouw ik in ieder geval als vertrouwelijk. Ik verstrek deze informatie niet aan anderen, ook niet binnen de organisatie, tenzij dit noodzakelijk is voor de uitoefening van mijn taak of ik daartoe wettelijk verplicht ben. Bij twijfel neem ik contact op met de opdrachtgever of de privacy officer binnen het organisatieonderdeel.

2. Toegang tot gebouwen

Ik gebruik de hulpmiddelen voor toegang tot locaties, apparatuur en ruimten van de organisatie uitsluitend voor het doel waarvoor deze aan mij ter beschikking zijn gesteld.

Ik probeer niet om onbevoegd toegang te krijgen tot locaties van de organisatie. Voor mij bestemde toegangsmiddelen behoud ik voor mijzelf en geef ik niet aan collega's of derden, tenzij daarover afspraken zijn gemaakt met de opdrachtgever en dit past in de bedrijfsvoering.

Bij vermissing, ontvreemding, misbruik of ander onrechtmatig gebruik van de mij verstrekte toegangspas, sleutels, tags, toegangscode's, apparatuur, software of andere middelen stel ik de daartoe aangewezen personen binnen het organisatieonderdeel waar ik werkzaam ben onmiddellijk daarvan in kennis.

Ik houd mij aan de regels die per locatie van de organisatie zijn gesteld ten aanzien van het ontvangen en begeleiden van bezoekers.

3. Omgang informatie

Ik laat geen stukken onbeheerd achter, ook niet op mijn bureau, in de ruimte of (thuis)werkplek waar ik werk, waarvan ik weet of zou kunnen weten dat deze vertrouwelijk zijn. Ik houd mij op mijn (thuis)werkplek aan de regels voor de beveiliging van informatie. Als ik vermoed dat er een inbreuk wordt gemaakt op de informatieveiligheid dan doe ik daarvan een melding aan mijn leidinggevende.

Documenten, e-mails, en overige zaken die niet voor mij bestemd zijn, zend ik onmiddellijk door aan het juiste adres of ik retourneer deze aan de afzender. Is het juiste adres noch de afzender bekend, dan vernietig ik ze. Ik beperk de inzage en/of het gebruik van vertrouwelijke gegevens tot wat nodig is voor de vervulling van mijn werkzaamheden (need-to-know principe).

4. Omgang bedrijfsmiddelen

Ik ga zorgvuldig om met alle mij ter beschikking gestelde bedrijfsmiddelen, zowel op mijn werkplek als elders waar ik bedrijfsmiddelen gebruik. Ik houd mij aan de geldende regels voor internet en e-mail gebruik en de huisregels van het organisatieonderdeel. Ik laat geen waardevolle bedrijfsmiddelen onbeheerd achter op mijn werkplek of elders waar ik bedrijfsmiddelen gebruik.

5. Integriteit

Ik gedraag mij integer, wat in ieder geval inhoudt dat ik mij houd aan de interne regels over integriteit en de huisregels van mijn organisatieonderdeel.

Als ik een misstand constateer, meld ik deze in eerste bij mijn opdrachtgever of diens superieur. Als ik anoniem wil blijven, zal ik gebruik maken van de 'Klokkenluiderregeling' en meld ik een geconstateerde misstand bij de vertrouwenspersoon bij mijn organisatieonderdeel.

Bij twijfel raadpleeg ik de coördinator integriteit of de centrale vertrouwenspersoon.

6. Omgangsvormen

Ik houd mij aan correcte omgangsvormen en ik houd mij aan de interne regels over ongewenst gedrag, omgangsvormen en de huisregels van mijn organisatieonderdeel.

Krijg ik te maken met ongewenste omgangsvormen dan kan ik mijn opdrachtgever raadplegen, dan wel de vertrouwenspersoon ongewenste omgangsvormen bij mijn organisatieonderdeel of de algemene vertrouwenspersoon. Wordt het probleem niet opgelost dan kan ik een klacht indienen bij de klachtencoördinator.

Ik verklaar verder in kennis te zijn gesteld van de inhoud van dit formulier en:

- mij te zullen houden aan alle in dit formulier genoemde (spel)regels;
- bekend te zijn met de verplichting melding te doen van elke schending van de geheimhoudingsplicht. Dit onverminderd hetgeen is bepaald in artikel 162 van het Wetboek van Strafvordering (geldend op 17 november 2015);
- kennis te hebben genomen van de bepalingen in het Wetboek van Strafrecht inzake geheimhouding (geldend op 20 april 2016), te weten de artikelen 2 tot en met 8, 23, 272 en 273;
- dat ik gedurende de duur van mijn inzet voor de werkzaamheden van de Samenwerkingsorganisatie en na beëindiging van deze werkzaamheden tegenover derden geheimhouding zal betrachten met betrekking tot alle (persoons)gegevens waarvan ik bij de uitvoering van voornoemde werkzaamheden kennis neem;
- dat ik de betekenis en het belang van die bepalingen heb begrepen.

Ondertekening medewerker

Plaats _____

Datum ____ / ____ / ____

Handtekening _____

Gezien door (namens de Samenwerkingsorganisatie)

Plaats _____

Datum ____ / ____ / ____

Naam _____

Functie _____

Handtekening _____

Toelichting Integriteits- en geheimhoudingsverklaring

Algemeen

Je hebt de geheimhoudingsverklaring ontvangen en moet deze ondertekenen. In de verklaring staan de wetsartikelen waar je je aan te houden hebt. Dit hoort erbij omdat we verplicht zijn om je goed en juridisch correct te informeren.

Wat staat er eigenlijk?

De gegevensverwerking (dit is ook het raadplegen van informatiesystemen als SUWI, BRP, financieel, personeelsinformatie- of zaaksysteem, direct of via een andere applicatie) is noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak en in het belang van betrokkene. Heb je de gegevens niet nodig, dan mag je ze ook niet raadplegen. Dit betekent ook dat je van een klant niet meer opvraagt, dan je voor je werk nodig hebt. We noemen dit ook wel “need-to-know”.

In de meeste applicaties is het toegangsbeheer per groep geregeld. Je hebt dus dezelfde rechten als je collega's, maar je hebt geen recht om gegevens te bekijken van een klant van een collega. Als je niet kunt uitleggen waarom je iets opvraagt, handel je waarschijnlijk in strijd met de bepalingen uit onder andere de Wbp (Wet bescherming persoonsgegevens).

Je weet dat alle opvragingen vastgelegd worden (logging) en dat dit regelmatig wordt gecontroleerd. Ook deze controle is een wettelijke verplichting.

Geheimhouding betekent ook dat je deze informatie niet met anderen deelt, behalve als je daar wettelijk toe verplicht bent (o.a. samenwerking Sociaal Domein). Concreet komt dit neer op de "clean desk policy" (geen vertrouwelijke informatie open en bloot laten liggen, ook niet op het scherm van je computer) en niet over klanten/burgers praten als dit niet nodig is. Moet dat wel, dan zorg je ervoor dat anderen niet kunnen meeluisteren. Is dat niet mogelijk, doe het dan zo dat niet herkenbaar is over wie (geen namen of adressen noemen) het gaat.

De wetgever neemt geheimhouding serieus. Zo bepaalt artikel 272 van het Wetboek van Strafrecht dat hiervoor een gevangenisstraf van maximaal één jaar of een geldboete van de vijfde categorie (per 01-01-2026 €110.000,-) kan worden opgelegd. In minder ernstige gevallen neemt de werkgever/opdrachtgever disciplinaire maatregelen, die kunnen variëren van een waarschuwing tot ontslag/beëindiging van de opdracht.

Wat betekent dat voor jou?

Zie het als de bepalingen in een contract. We vertrouwen elkaar, zijn integer en houden ons aan de afspraken en de gedragscode. Na ondertekening kijk je niet meer naar het contract. Alleen voor de hoge uitzondering waarin het mis gaat, moet je alles wel goed geregeld hebben.

De juiste wetteksten kun je hier vinden

- Ambtenarenwet artikel 125a;
- Wetboek van Strafrecht artikelen 2 tot en met 8, 23, 272 en 273;
- Wetboek van Strafvordering (geldend op 17 november 2015) artikel 162.

Nadere uitleg:

1. Geheimhouding

Vertrouwelijke informatie op schrift is te herkennen doordat er 'vertrouwelijk' op staat. Ook stempels of aantekeningen als 'geheim' en dergelijke kwalificeren een document als vertrouwelijk. Ook niet-schriftelijke informatie kan een vertrouwelijk karakter hebben, zoals interne uitspraken van het college, discussies of verschillen van mening.

2. Toegang tot gebouwen, apparatuur en kwetsbare ruimten

Met locatie wordt bedoeld elk gebouw waarin een onderdeel van de organisatie is gevestigd, of een plaats waar medewerkers werkzaam zijn, dus ook bedrijfsterreinen, kunstwerken, vervoermiddelen, etc.

Toegangsmiddelen zijn bijvoorbeeld toegangspassen, sleutels, tags, toegangscode's, wachtwoorden, apparatuur en software.

Voorbeelden van extra kwetsbare ruimten zijn: computer- en netwerkrumten, ruimten met communicatieapparatuur zoals telefooncentrales, archiefrumten, ruimten met toegang tot bedrijfsvoering gegevens ruimten waarin zich kluizen bevinden, werkplaatsen waar kostbare apparatuur aanwezig is.

3. Omgang informatie

Zoals onder het kopje 'Geheimhouding' al is aangegeven worden in ieder geval als vertrouwelijk beschouwd persoonsgegevens, financiële gegevens, klantgegevens, aanbestedingsgegevens en contractgegevens.

Voorbeelden van mogelijke beveiligingsmaatregelen zijn: clean desk, afsluiten kasten, aanzetten schermbeveiliging tijdens afwezigheid, regelmatig wijzigen van wachtwoorden, niet uitlenen van apparatuur of gegevensdragers aan derden.

4. Omgang bedrijfsmiddelen

Voorbeelden van bedrijfsmiddelen zijn: computers, (mobiele) telefoons, kantoorbehoeften, laptops, beamers, vervoermiddelen zoals dienstauto of dienstfiets.

Voorbeelden van ongewenst gebruik van inter-/intranet en e-mail zijn het surfen naar dubieuze websites, het openen van e-mail van totaal onbekende afzenders dan wel e-mail met een vreemde bijlage, het downloaden van muziekbestanden of software zonder licentie, etc.