

Bijlage bij 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 bijvoorbeeld de BRP, direct of via een andere applicatie) is noodzakelijk is voor de goede vervulling van je taken 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 cliënt 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 cliënt van een collega, tenzij hier nadrukkelijk afspraken over gemaakt zijn. Als je niet kunt uitleggen waarom je iets opvraagt, handel je waarschijnlijk in strijd met de wetten inzake gegevensbescherming.

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. Concreet komt dit neer op de z.g. Clean Desk Policy (geen vertrouwelijke informatie open en bloot laten liggen, ook niet op het scherm van je computer) en niet over cliënten/inwoners 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 staat in artikel 272 van het Wetboek van Strafrecht dat hiervoor een gevangenisstraf van maximaal 1 jaar of een geldboete van de vierde categorie kan worden opgelegd. In minder ernstige gevallen neemt de werkgever disciplinaire maatregelen, die kunnen variëren van een waarschuwing tot ontslag.

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.

De juiste wetteksten kun je hier vinden:

Wetboek van Strafrecht artikelen 2 tot en met 8, 23, 272 en 273

<http://wetten.overheid.nl/BWBR0001854/2018-01-01>

Wetboek van Strafvordering artikel 162

<http://wetten.overheid.nl/BWBR0001903/2018-01-01>

Wet Bescherming Persoonsgegevens

<http://wetten.overheid.nl/BWBR0011468/2017-07-01>

Algemene Verordening Gegevensbescherming

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/verordening_2016_-_679_definitief.pdf

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.

Daarnaast kan niet-schriftelijke informatie een vertrouwelijk karakter hebben, zoals interne uitspraken van het MT, discussies of verschillen van mening.

2. Toegang tot gebouwen, apparatuur en kwetsbare ruimten

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

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

Voorbeelden van extra kwetsbare ruimten zijn: computer- en netwerkruimten, ruimten met communicatieapparatuur zoals telefooncentrales, archiefruimten, ruimten met toegang tot bedrijfsvoeringsgegevens, 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 (bijzondere) persoonsgegevens, financiële gegevens, cliëntgegevens, 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.