Uitgangspunten sanctiebeleid bij oneigenlijk gebruik van Suwinet

Inleiding

Persoonlijke gegevens van burgers behoren bij gemeenten in veilige handen te zijn. Als gemeente wilt u dat burgers daarop kunnen vertrouwen. Daarom heeft u een autorisatiebeleid en vraagt u achteraf gebruikersrapportages en specifieke rapportages op. Tenslotte mogen medewerkers de gegevens in Suwinet alleen raadplegen als dit voor het werk noodzakelijk is. Toch kan uit analyse van de specifieke rapportage Suwinet, maar ook vanuit andere signalen, blijken dat gegevens mogelijk voor andere doeleinden zijn geraadpleegd. Als dat gebeurt, is het van belang een helder sanctiebeleid te hebben.

In deze notitie vindt u uitgangspunten die u helpen het besluitvormingsproces en het sanctiebeleid vorm te geven. Het blijft een eigen bevoegdheid van de desbetreffende organisatie om te bepalen of en zo ja welke straf wordt opgelegd in een concreet geval.

Uitgangspunten

De werkgever moet zich als een goed werkgever gedragen ten opzichte van zijn/ haar medewerkers. De medewerker op zijn beurt is gehouden om de belangen van zijn/ haar werkgever als een goed werknemer te behartigen. Dat houdt onder meer in, dat de werkgever ervan uit mag gaan, dat de medewerker de haar/ hem opgedragen werkzaamheden uitvoert overeenkomstig de bij zijn/ haar werkgever geldende regels en voorschriften, waaronder de regels en voorschriften voor juist Suwinet gebruik. Daarenboven geldt uiteraard, dat werkgever en werknemer zich houden aan de toepasselijke wet- en regelgeving (AVG).

Bepaalde medewerkers hebben uit hoofde van hun functie bij hun werkgever toegang tot het Suwinet. Zij worden daartoe door hun werkgever geautoriseerd. De werkgever gaat er vanuit en mag er van uit gaan, dat de medewerker zorgvuldig en juist omgaat met de hem/ haar verleende autorisatie.

Onder juist en zorgvuldig Suwinet gebruik wordt kort gezegd verstaan: “het raadplegen van het Suwinet gegevens door een medewerker is uitsluitend toegestaan als dat noodzakelijk is voor de uitoefening van zijn / haar functie bij zijn/ haar werkgever. De informatie, welke wordt verkregen in het kader van het raadplegen van Suwinet bij de uitoefening van zijn/ haar functie dient strikt zakelijk en vertrouwelijk te worden behandeld. Om hier vorm en inhoud aan te geven, kunt u de volgende uitgangspunten hanteren.

1. Werkgever moet zorgen voor voldoende adequate voorlichting aan medewerkers omtrent het beleid van de werkgever bij gegevensraadplegingen door zijn/ haar medewerkers en over de mogelijke gevolgen voor de rechtspositie van de medewerkers bij oneigenlijke raadplegingen.
2. Werkgever maakt aan zijn/haar medewerkers voldoende duidelijk dat het raadplegen van gegevens buiten opvragingen welke noodzakelijk zijn voor de uitoefening van de functie, strikt verboden is. Dat geldt voor alle niet-werk gerelateerde opvragingen, waaronder onder meer ook de eigen gegevens en gegevens van gezins- en familieleden.
3. Werkgever maakt aan zijn/ haar medewerkers voorts voldoende duidelijk – onder meer in een gedragscode en in een door de medewerker te ondertekenen

geheimhoudingsverklaring/ verklaring van integriteit -, dat het raadplegen van gegevens buiten opvragingen, welke noodzakelijk zijn voor de uitoefening van de functie plichtsverzuim is en kan leiden tot een disciplinaire maatregel en aangifte. Daarbij is ontslag op staande voet/ disciplinair strafontslag, afhankelijk van de toepasselijke rechtspositieregeling niet uitgesloten.

4. Alle feiten en omstandigheden, inclusief de belangen van zowel werkgever en de desbetreffende werknemer moeten door werkgever worden betrokken en gewogen bij de besluitvorming. Het opleggen door werkgever van een passende disciplinaire maatregel-strafmaat- in een concrete situatie, is maatwerk.
5. Het proces van besluitvorming moet voldoende zorgvuldig en voldoende voortvarend zijn. Voortvarendheid betekent: er is geen sprake van nodeloos (of: niet te verklaren) tijdsverlies.
6. Incidenteel, niet stelselmatig, oneigenlijk raadplegen van Suwinet leidt in beginsel tot het opleggen van een waarschuwing of schriftelijke berisping, afhankelijk van de toepasselijke rechtspositieregeling. Bij incidenteel oneigenlijk raadplegen is in dit verband sprake van een op zichzelf staand incident.
7. Incidenteel oneigenlijk raadplegen van het Suwinet, waarbij de daaruit verkregen informatie wordt gebruikt ten nadele van de geraadpleegde persoon en/of ten voordele van de raadpleger zelf en/ of (een) derde(n) leidt tot een zwaardere disciplinaire maatregel dan waarschuwing/ berisping, waarbij ontslag op staande voet/ strafontslag en aangifte niet wordt uitgesloten.
8. Onder “stelselmatig oneigenlijk Suwinet raadplegen” wordt verstaan: het veelvuldig oneigenlijk raadplegen van Suwinet, anders gezegd, meer dan een enkel incident. Het stelselmatig oneigenlijk Suwinet raadplegen door een medewerker is naar aard en inhoud ernstig plichtsverzuim. Dit plichtsverzuim leidt tot het opleggen van een disciplinaire maatregel, die qua zwaarte passend is ten opzichte van het gepleegde verzuim. Ontslag op staande voet c.q. disciplinair strafontslag is mogelijk. Dit geldt zeker als daarbij de daaruit verkregen informatie door de raadpleger wordt gebruikt ten nadele van de geraadpleegde persoon en /of wordt gedeeld met één of meerdere anderen.
9. Bij het bepalen van de strafmaat bij stelselmatig oneigenlijk Suwinet gebruik kunnen de volgende uitgangspunten worden betrokken en meegewogen:
   - Als de verkregen informatie extern is gedeeld met (een) ander(en) en/of heeft geleid tot eigen voordeel en/of voordeel voor (een) ander(en) leidt dat tot ontslag op staande voet.
   - “Persoonlijke omstandigheden”, zoals de duur van het dienstverband, de leeftijd van de betrokken medewerker, de wijze van diens functioneren en diens positie op de arbeidsmarkt zijn in dat geval van onvoldoende gewicht voor een minder zware sanctie.