

Tien gouden regels bij beveiliging van persoonsgegevens

Voor het werken met en de omgang met persoonsgegevens zijn vanuit de overheid een aantal regels opgesteld, die zijn verwoord in verschillende wet- en regelgeving. Concreet kunnen deze regels als volgt worden vertaald:

1. Beheren van wachtwoorden

De gebruiker moet het door de administrator uitgegeven wachtwoord wijzigen zodra de eerste inlog plaatsvindt. Vervolgens vervalt dat wachtwoord iedere keer na 90 dagen. De gebruiker heeft dus het eigen beheer over het wachtwoord. Zodra een medewerker de gemeente verlaat, wordt het account verwijderd.

2. Melden van beveiligingsincidenten

Het is belangrijk dat beveiligingsincidenten worden gemeld bij de applicatiebeheerder. Vervolgens wordt de afdeling Systeembeheer ingeschakeld om dat incident te onderzoeken. Voorbeelden van incidenten zijn: een virusmelding op het systeem of een inbraak of poging tot inbraak.

3. Geheimhoudingsplicht

Binnen Werkplein Fivelingo wordt met persoonsgegevens gewerkt. Voor het werken met en de omgang met persoonsgegevens zijn vanuit de overheid een aantal regels opgesteld, die zijn verwoord in de Wet bescherming persoonsgegevens (WBP). In de wet SUWI en in de CAO zijn geheimhoudingsbepalingen opgenomen, waarin wordt aangegeven dat de persoonsgegevens niet verder bekend mogen worden gemaakt dan voor de uitoefening van de functie noodzakelijk is.

4. Gedragscode internet- en emailgebruik

De gemeente hanteert een protocol voor gebruik van email en internet. In dit protocol is aangegeven hoe de medewerkers behoren om te gaan met email en internet op de werkplek. Tevens bevat dit protocol regels voor de manier waarop het gebruik van externe email en internet wordt geobserveerd. Het protocol is voor alle medewerkers van de gemeente te raadplegen op het gemeentelijke Intranet.

5. Kennisnemen van het informatiebeveiligingsbeleid

Het binnen Werkplein Fivelingo geldende informatiebeveiligingsbeleid (inclusief instructies en protocollen) is op iedereen binnen de afdeling van toepassing die gebruik maakt van Suwinet-Inkijk. Alle gebruikers hebben een exemplaar van de beveiligingsnota ontvangen en ook nieuwe medewerkers/gebruikers zullen via het afdelingshoofd een exemplaar ontvangen. Gebruikers van Suwinet-Inkijk moeten weten dat over hen gegevens worden vastgelegd en verzameld. Dit is een belangrijk onderdeel van de privacybescherming ten opzichte van deze medewerkers. In de beveiligingsnota is hier uitgebreid aandacht aan besteed. Jaarlijks, bij de evaluatie van het Beveiligingsnota, wordt dit onderwerp geagendeerd voor het werkoverleg.

6. Gegevensverstrekking aan derden via de telefoon

Het uitgangspunt is dat er met terughoudendheid aan verzoeken om telefonische informatie over betrokkenen wordt tegemoetgekomen. Het voeren van telefoongesprekken brengt namelijk de risico's met zich mee dat de identiteit van de gesprekspartner verkeerd wordt vastgesteld of dat persoonsgegevens worden verstrekt aan personen die geen recht op informatie hebben. In principe wordt er dan ook geen telefonische informatie over klanten verstrekt aan personen of instanties die beweren namens betrokkene te bellen. In die gevallen kan er een schriftelijk verzoek worden ingediend, voorzien van een machtiging. Bij een verzoek om telefonische informatieverstrekking van een ketenpartner wordt de verzoeker teruggebeld via het algemene nummer van de (vestiging van de) ketenpartner met het verzoek te worden doorverbonden. Dit terugbellen kan achterwege blijven indien afkomstig van een vaste contactpersoon.

7. 'Clean desk' en 'clear screen' policy

De vertrouwelijke omgang met persoonsgegevens houdt onder andere in dat elke werkplek zodanig is ingericht, dat onbevoegden niet de beschikking kunnen krijgen over deze informatie. Vertrouwelijke gegevens mogen niet onbeheerd op het bureau achterblijven. Dossiers worden bewaard in een kast die na werktijd wordt gesloten. Bezoekers dienen zich bij binnenkomst in het gemeentehuis eerst te melden bij de receptie. De kans is derhalve gering dat onbevoegden zonder te worden opgemerkt toegang krijgen tot de werkplek van de medewerkers. Clear screen betekent dat het werkstation moet worden vergrendeld met behulp van schermbeveiliging (met wachtwoord). De screensaver is zodanig ingesteld dat na een x-aantal minuten de schermbeveiliging intreedt. Dit is door de afdeling Systeembeheer voor iedere medewerker standaard ingesteld.

8. Geen vertrouwelijke gegevens in de prullenbak

De correcte omgang met vertrouwelijke gegevens – waaronder persoonsgegevens – is erg belangrijk binnen Werkplein Fivelingo. Ook het vernietigen van deze gegevens moet op een veilige manier plaatsvinden. Daarom zijn er op iedere kamer speciale zakken geplaatst, waarin het te vernietigen materiaal verzameld wordt. De verzamelde vertrouwelijke gegevens worden regelmatig aangeleverd bij het vernietigingsbedrijf. Vertrouwelijke gegevens dienen niet terecht te komen in een prullenbak of een bak die bestemd is voor oud papier.

9. Aanspreken van onbekende personen

In het geval dat een medewerker van Werkplein Fivelingo een voor hem/haar onbekende persoon in de gang van de afdeling tegenkomt waar officieel geen publiek zonder begeleiding mag komen, dient de medewerker deze persoon aan te spreken, zichzelf voor te stellen en de persoon in kwestie te vragen wat hij/zij hier doet. Personen die niet bevoegd zijn om zich op deze plek te bevinden worden hierdoor op deze overtreding gewezen. Het is de taak van de medewerker om hun beleefd maar duidelijk de weg naar het publieke gedeelte van het gebouw te wijzen en ze daarnaartoe te begeleiden.

10. De dagelijkse werkzaamheden vs. Informatiebeveiliging

Informatiebeveiliging is uitermate belangrijk voor het werk binnen Werkplein Fivelingo waar veelvuldig met privacygevoelige informatie wordt gewerkt en hoort dan ook bij de professionele en bekwame uitvoering van het werk. Ook cliënten vertrouwen op een zorgvuldige wijze van verwerken van hun gegevens. Reden waarom middels het werkoverleg geregeld aandacht voor dit onderwerp besteed dient te worden.