

Bijlage 1 – Regels werken met persoonsgegevens

In verschillende wet- en regelgeving zijn regels vastgelegd voor het werken met persoonsgegevens. De belangrijkste regels zijn:

1. Beheren van wachtwoorden

De gebruiker moet het door de applicatiebeheerder uitgegeven wachtwoord wijzigen zodra de eerste inlog plaatsvindt. Daarna vervalt het wachtwoord iedere keer na 8 weken. De gebruiker heeft dus het eigen beheer over het wachtwoord. Zodra een medewerker de dienst verlaat, wordt het account verwijderd. Wanneer het account 56 dagen niet wordt gebruikt, wordt het wachtwoord geblokkeerd.

2. Melden van beveiligingsincidenten

Het is belangrijk dat beveiligingsincidenten worden gemeld bij de gebruikersbeheerder Suwinet-Inkijk. Daarna wordt de Service Desk van de gemeente Berkelland ingeschakeld om het incident te onderzoeken. Voorbeelden van incidenten zijn: een virusmelding op het systeem of een inbraak of poging tot inbraak.

3. Geheimhoudingsplicht

Binnen Fijnder wordt met persoonsgegevens gewerkt. Voor het werken met persoonsgegevens zijn vanuit Europa en het Rijk een aantal regels opgesteld, die zijn vastgelegd in de Algemene verordening gegevensbescherming. In de wet SUWI en in de Ambtenarenwet zijn geheimhoudingsbepalingen opgenomen, waarin wordt aangegeven dat de persoonsgegevens niet verder bekend mogen worden gemaakt dan voor de uitoefening van de functie noodzakelijk is. De medewerker Fijnder ondertekent bij indiensttreding een verklaring omtrent integriteit en geheimhouding.

4. Kennisnemen van het informatiebeveiligingsbeleid

Het binnen Fijnder geldende informatiebeveiligingsbeleid is op iedereen die gebruik maakt van Suwinet-Inkijk van toepassing. 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 het aansluitbeleid gebruik Suwinet-Inkijk is hier aandacht aan besteed.

5. Gegevensverstrekking aan derden via de telefoon

In principe wordt er geen telefonische informatie over cliënten 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 (UWV, UWV-Werkbedrijf, gemeente) 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 bij een vaste contactpersoon.

6. Opgeruimd bureau en leeg beeldscherm

Opgeruimd bureau houdt onder andere in dat elke werkplek zodanig is ingericht, dat onbevoegden niet de beschikking kunnen krijgen over vertrouwelijk- en/of privacygevoelige informatie. Vertrouwelijke gegevens mogen niet onbeheerd op het bureau achterblijven. Cliëntdossiers worden bewaard in een kast die na werktijd wordt afgesloten.

Bij het verlaten van de werkplek betekent dat het werkstation actief moet worden vergrendeld met behulp van schermbeveiliging (met wachtwoord). De screensaver is zodanig ingesteld dat bij geen gebruik na 10 minuten de schermbeveiliging automatisch intreedt.

7. Geen vertrouwelijke gegevens in de prullenbak

De correcte omgang met vertrouwelijke gegevens – waaronder persoonsgegevens – is erg belangrijk binnen Fijnder. Ook het vernietigen van deze gegevens moet op een veilige manier plaatsvinden. Alle te vernietigen vertrouwelijke gegevens, waaronder cliëntinformatie moeten worden gedeponeerd in de afgesloten containers.

8. Aanspreken van onbekende personen

Bezoek meldt zich altijd aan de publieksbalie. Een externe wordt opgehaald door de medewerker waarmee de afspraak is. In het geval dat een medewerker van Fijnder een voor hem/haar onbekende persoon in het kantoor gedeelte van Fijnder tegenkomt spreekt de medewerker deze persoon aan, stelt zichzelf voor en vraagt de persoon in kwestie wat hij/zij hier doet. Personen die niet bevoegd zijn om zich op deze plek te bevinden worden hierop aangesproken. Het is de taak van de betreffende medewerker om hun beleefd, maar duidelijk de weg naar het publieke gedeelte van het gebouw te wijzen en ze daarnaartoe te begeleiden.

9. De dagelijkse werkzaamheden en informatiebeveiliging

Iedere medewerker moet zich er bewust van zijn dat informatiebeveiliging belangrijk is voor de uitvoering van zijn/haar taken. Zorgvuldig omgaan met privacygevoelige informatie is onderdeel van een professionele en bekwame uitvoering van het werk.