

Aandacht voor privacy en Informatieveiligheid



Omgaan met persoonsgegevens van cliënten en collega's.
Informatie en praktische tips voor medewerkers van Surplus!

Even voorstellen



**Tjek
Dubbel**



**Ben
Veilig**



**Bennie
Veilig**



Boef

Onze ambassadeur Tjek Dubbel gaat op pad om je bewust te maken van het belang van privacy en informatieveiligheid. Tjek Dubbel wordt bijgestaan door Ben Veilig, Bennie Veilig en Boef. Je gaat hen vaker zien en zeker nog eens ontmoeten.

Lees dit boekje goed door

Daarna weet je hoe je met vertrouwelijke gegevens om moet gaan.
Bewaar dit boekje als je persoonlijke naslagwerk.



Voorwoord

Surplus staat voor meerwaarde. Voor extra. Wij willen de verwachtingen van onze klanten overtreffen. Onze focus ligt op kwaliteit, persoonlijke aandacht voor klanten en oprechte betrokkenheid van medewerkers en vrijwilligers. Dat lukt ons alleen als we samen duidelijke afspraken maken over hoe we met elkaar omgaan.

Wij vinden het belangrijk dat we elkaars **privacy** respecteren. We gaan zorgvuldig om met de persoonsgegevens van onze klanten, hun vertegenwoordigers, bezoekers en uiteraard ook van onze medewerkers en vrijwilligers.

Dit boekje helpt je met antwoorden over gebruik van je ICT-voorzieningen, e-mail en internetgebruik, omgang met persoonsgegevens, zorgvuldig afhandelen van datalekken en nog veel meer. Allemaal informatie die nodig is om op een plezierige manier met elkaar te kunnen samenwerken en om onze cliënten, hun vertegenwoordigers en bezoekers de zorg te kunnen verlenen, die zij van ons mogen verwachten. En zelfs nog een beetje meer.

We rekenen op je medewerking.

Anton van Mansum
Jan Verbaal
Anthonie Maranus

raad van bestuur Surplus

Vragen over privacy en informatieveiligheid

Aandacht voor privacy	6
Wat is 'verwerken van persoonsgegevens'?	8
Welke privacyrechten hebben cliënten?	8
Moet ik toestemming vragen om persoonsgegevens te verwerken?	10
Waar bewaar je cliëntgegevens?	12
Hoe lang mag je cliëntgegevens bewaren?	12
Hoe gebruik je internet veilig?	16
Hoe ga je om met nepmails?	18
Wat zijn datalekken en waarom moet je die melden?	20
Hoe ga je om met de bezoekers op locaties van Surplus?	22
Welke rechten hebben medewerkers en werkgever?	24
Belangrijke privacy tips	27

Aandacht voor privacy

Aandacht voor privacy is belangrijk. Onzorgvuldig- of nalatig handelen met gevoelige persoonsgegevens kan leiden tot grote schade. Voor onze klanten, hun vertegenwoordigers, onze medewerkers, onze vrijwilligers én ook onze organisatie. **Aandacht voor privacy** is vanzelfsprekend in ons dagelijks handelen. Iedereen heeft recht op goede bescherming van zijn persoonsgegevens en bij Surplus doen wij dit volgens de privacy-wetgeving. Belangrijke privacywetten zijn de Algemene Verordening Gegevensbescherming (AVG) en de wet Cliëntenrechten bij elektronische verwerking van gegevens.

Wat zijn persoonsgegevens?

Een persoonsgegeven is **alle informatie die over een persoon gaat**, zoals naam, adres, foto of inloggegevens. Ook informatie die te herleiden is naar een persoon, is een persoonsgegeven. Je kunt bijvoorbeeld met postcode én huisnummer al achterhalen waar iemand woont.

Gevoelige of **bijzondere persoonsgegevens** krijgen extra bescherming. Informatie over gezondheid, ras, seksuele voorkeur, financiën en godsdienst zijn voorbeelden van gevoelige persoonsgegevens. Bij Surplus verwerken wij veel (bijzondere) persoonsgegevens en hebben dus een grote verantwoordelijkheid om deze gegevens goed te beschermen.

De functionaris gegevensbescherming houdt bij Surplus toezicht op het naleven van de privacywetgeving. De functionaris is vraagbaak voor jouw vragen en vragen van cliënten. Mail je vraag naar privacy@surplus.nl.

Verwerken van (bijzondere) persoonsgegevens



Wat is ‘verwerken van persoonsgegevens’?

De privacywetgeving is van toepassing als er sprake is van het verwerken van persoonsgegevens. Hieronder valt iedere bewerking, zoals het opslaan, verzamelen, wijzigen, opvragen, raadplegen, wissen of verspreiden van persoonsgegevens. Je kunt ervan uitgaan dat de regels uit de AVG gelden als je, op welke manier dan ook, in aanraking komt met persoonsgegevens.

Welke privacyrechten hebben cliënten?

De privacywetgeving geeft cliënten een aantal rechten:

- Het recht op inzage in de persoonsgegevens die van hen verwerkt worden.
- Het recht op informatie over welke gegevens van hen verwerkt worden en hoe met deze gegevens wordt omgegaan.
- Het recht om hun persoonsgegevens eenvoudig over te dragen aan een andere zorgaanbieder.
- Het recht om hun gegevens te laten verwijderen, te corrigeren en af te schermen.
- Het recht om bezwaar in te dienen als zij van mening zijn dat hun persoonsgegevens niet juist worden verwerkt.

De privacyrechten van cliënten staan beschreven in de **verklaring bescherming persoonsgegevens**. Hiervan zijn meerdere versies. Een versie voor cliënten van zorg en één voor cliënten van welzijn. Ook is er een versie voor medewerkers van Surplus. Deze verklaringen staan op de website van Surplus en Surplusnet

Tip: Cliënten hebben inzagerecht, houd de informatie in het cliëntdossier daarom altijd zakelijk!

Cliënten hebben recht op inzage in hun gegevens. Houd daar rekening mee!



Moet ik toestemming vragen om persoonsgegevens te verwerken?

In veel gevallen moet je toestemming vragen als je persoonsgegevens van medewerkers of cliënten wilt verwerken. Als er een wettelijke verplichting is om persoonsgegevens te verwerken, hoef je geen toestemming te vragen. Dit is bijvoorbeeld het geval bij het aanleggen van een zorgdossier van cliënten. Ook hoef je geen toestemming te vragen als in de zorgovereenkomst al afspraken zijn gemaakt over het verwerken van persoonsgegevens. Het is dus belangrijk dat je goed op de hoogte bent van de inhoud van de zorgverleningsovereenkomst.

Toestemming vraag je altijd schriftelijk. Hierbij geef je duidelijk aan waarvoor toestemming wordt gevraagd. Ook geef je aan dat de toestemming altijd mag worden ingetrokken en hoe cliënten dit kunnen doen. Het toestemmingsformulier moet voorzien zijn van een datum en in het dossier van de cliënt worden opgeslagen.

Tip: Als je foto's of video's wilt maken van cliënten heb je altijd toestemming van de cliënt nodig. Als je twijfelt, overleg dan met de functionaris voor gegevensbescherming.

**Altijd vooraf toestemming vragen.
Ook als je een foto of video wilt maken!**



Waar bewaar je cliëntgegevens?

Cliëntgegevens sla je op **in het elektronisch cliëntendossier** (ECD). Dit is de enige plaats waar je cliëntgegevens mag opslaan, omdat ze daar afdoende worden beveiligd. Een papieren archief is moeilijk actueel te houden en gevoelig voor verlies. Dit doen we dus niet meer. Ook slaan we gegevens niet op algemeen toegankelijke netwerkschijven op. Alleen met goed beveiligde opslag kunnen we verantwoording afleggen over het zorgvuldig omgaan met persoonsgegevens van cliënten.

Bij Welzijn wordt geen gebruik gemaakt van het ECD, maar van Regas. Cliëntgegevens van Welzijn worden dus altijd in Regas opgeslagen.

Tip: Als cliëntinformatie niet in het officiële elektronische cliëntdossier zit, plaats dit daar dan alsnog. **Vernietig de oude (papieren) versie** in een versnipperaar of beveiligde documentenbak. Twijfel je? Overleg dan met je manager of de functionaris voor gegevensbescherming.

Hoe lang mag je cliëntgegevens bewaren?

De wettelijke termijn voor het bewaren van medische gegevens is 15 jaar, nadat het cliëntendossier is afgesloten of de behandelrelatie is beëindigd. **Als de bewaartermijn is verlopen, worden de gegevens vernietigd.** Voor overige gegevens geldt dat deze niet langer dan noodzakelijk mogen worden bewaard. In Regas bewaren we de dossiers drie jaar.

Berg vertrouwelijke documenten goed op en vernietig ze als ze niet meer nodig zijn!



Hoe gebruik je e-mail en social media?

Om onze werkzaamheden goed uit te voeren maken we vrijwel allemaal dagelijks gebruik van internet, e-mail en smartphone. Onderstaand enkele richtlijnen voor veilig gebruik hiervan.

Gebruik e-mail

1. Verstuur zo min mogelijk e-mail. Verwijs bij voorkeur naar de locatie waar informatie staat. Dit geldt zeker voor cliëntgegevens, die in het ECD of Regas staan.
2. Gebruik altijd beveiligde mail als je persoonsgegevens of andere vertrouwelijke gegevens naar een extern adres moet sturen. Informeer voor de mogelijkheden van beveiligd mailen bij de servicedesk ICT.
3. Verstuur e-mail nooit anoniem.
4. Stuur je een mail naar een groep privé adressen? Maak dan gebruik van bcc zodat niemand gegevens van de hele groep ziet.

Gebruik social media

1. Het is lastig om op social media onderscheid te maken tussen privé en werk. Denk daarom goed na, voordat je berichten plaatst.
2. Plaats in ieder geval nooit zonder toestemming informatie over cliënten en collega's of vertrouwelijke informatie op sociale media.
3. De inhoud van je profiel op sociale media is volledig je eigen verantwoordelijkheid.
4. Surplus ondersteunt de open dialoog en uitwisseling van ideeën en het delen van kennis.
5. Medewerkers en vrijwilligers die iets publiceren op een externe website of sociale media die niet van Surplus zijn, moeten kenbaar maken dat dit op persoonlijke titel is.
6. Ben terughoudend met reacties op een online berichtgeving over Surplus. Stem dit altijd af met je manager of afdeling communicatie. Als je reageert, vermeld dan altijd je naam en functie.

Let goed op als je vertrouwelijke mail verstuurt!



Hoe gebruik je internet veilig?

Gebruik internet

1. Gebruik internet, e-mail en smartphone alleen voor activiteiten die nodig of gewenst zijn in het belang van je werkzaamheden.
2. Respecteer bij het gebruik van internet alle wettelijke voorschriften, bijvoorbeeld auteursrecht van teksten en foto's.
3. We gaan op een respectvolle manier om met onze cliënten, bezoekers, collega's en vrijwilligers.
4. Geen enkele vorm van onfatsoenlijk gedrag, pesten, (seksuele) intimidatie, discriminatie, agressie en geweld wordt geaccepteerd.
5. Bekijk, vertoon, download en/of verspreid geen bestanden die het aanzien van de organisatie schade (kunnen) berokkenen of de grenzen van fatsoen overschrijden.
6. Gebruik nooit openbare Wifi hotspots, of hotspots waarvan je niet zeker weet dat deze goed beheerd en goed beschermd zijn.

Controle op gebruik internet

Verkeerd gebruik van internet kan leiden tot grote schade voor Surplus. Om die reden mag Surplus als werkgever controles uitvoeren. Controles hebben de volgende redenen als doel:

- Beoordelen van het functioneren van de medewerker
- Voorkomen van negatieve publiciteit
- Tegengaan van seksuele intimidatie
- Controleren van bedrijfsgeheimen
- Beveiligen van systemen en netwerken
- Beheersen van kosten en capaciteit
- Tegengaan van discriminatie

Hoe gebruik je de ICT-voorzieningen?

1. Installeer of update niet zelf software op apparatuur van Surplus. Dit wordt altijd gedaan door de Servicedesk ICT.
2. Gebruik je gebruikersnaam en wachtwoord niet op Surplus-vreemde apparatuur.
3. Deel geen gevoelige **gegevens** via WeTransfer, Dropbox, OneDrive, Google Drive of vergelijkbare toepassingen.
4. Vergrendel je computer/laptop als je de werkplek verlaat, zodat schermbeveiliging wordt ingeschakeld.
5. Let altijd goed op je laptop en smartphone. Laat deze nooit onbeheerd achter. Zeker niet in je auto.
6. Is je computer of smartphone gestolen? Meld dit dan direct bij Servicedesk ICT. Zij blokkeren dan direct je account, zodat de informatie is beschermd.
7. Surplus kent complexe wachtwoorden. Onze wachtwoorden zijn 8 posities en bevatten hoofdletters, kleine letters, cijfers en vreemde tekens.
8. Je wachtwoord is persoonlijk en geef je aan niemand. Een wachtwoordkluis helpt als je veel wachtwoorden moet onthouden.
9. Koppel geen andere apparaten, zoals USB-sticks, externe harde schijven en/of camera's aan je computer.
10. Laat nooit een afdruk onbeheerd bij de printer achter. Haal je afdruk direct op.
11. Meld storingen, onregelmatigheden, inbreuken op de beveiliging, ongeautoriseerd gebruik, etc. direct aan de systeembeheerder.
12. Breng zonder toestemming van werkgever geen vertrouwelijke informatie, of informatie waar intellectueel eigendomsrecht op rust, buiten het bedrijfsnetwerk van Surplus.

Hoe ga je om met nepmails?

In je mailbox zit regelmatig een e-mail van een afzender die je niet kent. Of met inhoud die je niet vertrouwt. De kans is dan groot dat je met zogenaamde phishing mail, een virus of andere aanval te maken hebt. Let dan goed op!

- Klik nooit op links, voordat je zeker weet dat de mail vertrouwd is.
- Soms wordt gevraagd naar je wachtwoord of pincode. **Geef deze nooit!** Er wordt per mail door niemand, ook niet door Servicedesk ICT om een wachtwoord gevraagd.
- Neem bij twijfel contact op met Servicedesk ICT, servicedeskict@surplus.nl of 0168-331899.

Let op! Heb je een pakketje bij een webshop besteld en krijg je even later een mail met daarin een link om je pakketje te volgen. De kans is groot dat dit een phishingmail is. Hackers volgen je gedrag op internet en sturen je deze nepmail of je gegevens te ontfutselen.

Bescherm persoonsgegevens zorgvuldig!



Wat zijn datalekken en waarom moet je die melden?

Wie werkt, maakt fouten. Daarom kan het gebeuren dat persoonsgegevens verloren gaan. We noemen dat een datalek.

Wat is een datalek?

Als bij een incident persoonsgegevens zijn betrokken, die (mogelijk) zijn ingezien door onbevoegde personen of verloren zijn geraakt, dan noemen we dat een datalek. Voorbeelden zijn:

- dossier met cliëntgegevens is kwijtgeraakt
- kopie van paspoort met burgerservicenummer is zoek
- laptop of telefoon is gestolen
- behandelrapportage is naar verkeerd adres verstuurd
- e-mail met persoonsgegevens is naar verkeerd e-mailadres gestuurd

Direct melden

Denk jij dat er sprake is van een datalek? Meld dit dan direct aan datalek@surplus.nl. De servicedesk krijgt deze melding binnen en stuurt je het meldingsformulier toe. Vul dit meldingsformulier meteen in en stuur het terug. De servicedesk zorgt ervoor dat het incident snel wordt opgepakt en afgehandeld.

Leermoment

Het melden van datalekken is een goede manier om het beschermen van persoonsgegevens bij Surplus steeds verder te verbeteren. Dus zie je iets wat niet goed gaat en waar persoonsgegevens een rol spelen? Stuur dan een mail naar datalek@surplus.nl. Wij rekenen op je medewerking!



Meld een datalek direct, dan kunnen we snel actie ondernemen!



Het is wettelijk verplicht om datalekken binnen 72 uur te melden aan de Autoriteit Persoonsgegevens.

Hoe ga je om met de bezoekers op locaties van Surplus?

De locaties van Surplus zijn openbaar en vrij toegankelijk. Gastvrijheid voor de bezoekers van onze bewoners is van groot belang. Dit vraagt van alle medewerkers **extra alertheid** op de bescherming van persoons- en bedrijfsgegevens.

- Let op je eigen werkplek én die van je collega's
- Zorg ervoor dat **vertrouwelijke documenten niet in het zicht** liggen
- Wees alert op ongenode gasten. Tref je iemand aan die niet op de locatie thuishoort, spreek hem of haar aan.
- Houd een oogje in het zeil.

Zie je iemand, waarvan je denkt dat hij of zij niet op de locatie hoort, spreek hem of haar dan hierop aan.



Welke rechten hebben medewerkers?

Rechten van de medewerker

- Jij mag aan de afdeling P&O vragen om een volledig overzicht van de persoonsgegevens die wij van je verwerken en bewerkt hebben. Je verzoek wordt binnen vier weken beantwoord.
- Je mag de afdeling P&O vragen je persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen. Dit kan als deze gegevens feitelijk onjuist zijn, voor het doel onvolledig, niet relevant of in strijd met een wettelijk voorschrift zijn. Ook dit verzoek wordt binnen vier weken beantwoord.

De privacyrechten van medewerkers staan beschreven in de verklaring bescherming persoonsgegevens. Deze verklaring kun je vinden op Surplusnet.

**Als medewerker heb je recht om je
persoonsgegevens in te zien!**



Ga zorgvuldig om met persoonsgegevens!



Belangrijke privacy tips

1. Cliëntgegevens sla je alleen op in het **elektronisch cliëntendossier** (zorg) of **Regas** (welzijn).
2. Gegevens van medewerkers en vrijwilligers sla je alleen op in Beaufort.
3. Uitwisselen van cliëntgegevens doe je bij voorkeur via het **elektronisch cliëntendossier** of **Regas**.
4. Persoonsgegevens worden **nooit op de netwerkschijven** opgeslagen.
5. Uitwisseling van cliëntgegevens met zorgverleners is bij voorkeur schriftelijk (wel digitaal). Mondelinge uitwisseling leidt tot interpretatiefouten of invoerfouten.
6. Verpleegkundige overdracht tussen ziekenhuis en Surplus gaat altijd met gestandaardiseerde berichten.
7. Maak gebruik van de **beveiligde portalen** van de zorg-aanbieders. Let op dat de verbinding veilig is (slotje in de balk).
8. Is het echt noodzakelijk om **cliëntinformatie te mailen**? Dan gebruik je beveiligde mail.
9. Je **gebruikt nooit sociale media**, zoals WhatsApp om persoonsgegevens uit te wisselen.
10. Verstuur je cliëntgegevens per post? Dan krijgt dit het kenmerk **persoonlijk** en wordt de brief **aangetekend** verzonden.
11. Houd **geen papieren archief** bij met persoonsgegevens.
12. Als documenten **niet meer nodig** zijn, dan worden ze **vernietigd**.
13. Neem **nooit persoonsgegevens** van cliënten of medewerkers **mee naar huis**.

Aandacht voor privacy en informatieveiligheid



Meer informatie

functionaris voor gegevensbescherming.

E-mail: privacy@surplus.nl.

ICT-voorzieningen en beveiligingsmaatregelen

E-mail: servicedeskict@surplus.nl.

Verwerken van je eigen persoonsgegevens

[afdeling P&O.](#)

Melden datalekken

Servicedesk ICT

E-mail: datalek@surplus.nl.