SEVERINUS
BIJZONDER IN SAMENLEVEN

AANDACHT VOOR
PRIVACY

AANDACHT VOOR PRIVACY

Zorgvuldig omgaan met persoonsgegevens is een voorwaarde voor een goede samenwerking. Privacy is daarom belangrijk voor jou, je collega's en onze cliënten. Daar hecht Severinus veel waarde aan.

De Algemene Verordening Gegevensbescherming (AVG) is de opvolger van bestaande privacywetten. Deze nieuwe regelgeving gaat een stap verder in de bescherming in de privacy van personen.

In dit boekje geven we je achtergrondinformatie over de AVG en bieden we praktische tips om zorgvuldig met privacy om te kunnen gaan.

Bedankt voor jullie medewerking!

INHOUDSOPGAVE

PRIVACY
HET BESCHERMEN VAN PERSOONSGEGEVENS

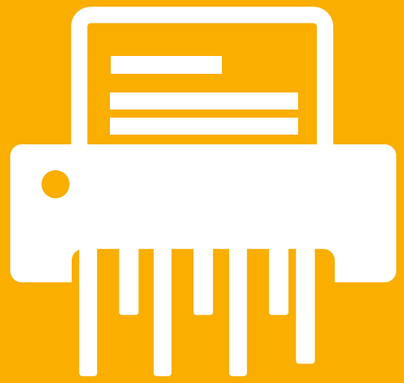
De AVG geeft richtlijnen en regels om de privacy van personen te beschermen. De wet geldt voor iedereen die op een of andere manier omgaat met persoonsgegevens. De AVG heeft betrekking op één of andere manier van verwerking: dus wanneer je persoonsgegevens raadpleegt, bewerkt, opslaat, verzamelt, print of verspreidt, heb je er al mee te maken.

PERSOONSGEGEVENS

- Dit betreft alle informatie die kan leiden naar een persoon, zoals een naam, adres of geboortedatum. Met alleen een postcode én een huisnummer kun je bijvoorbeeld al achterhalen waar iemand woont.
- Onder persoonsgegevens vallen niet de informatie over organisaties en gegevens van overleden personen.
- Er zijn bijzondere persoonsgegevens die extra bescherming krijgen, zoals informatie over gezondheid, ras, seksuele voorkeur of godsdienst. Severinus verwerkt veel gezondheidsgegevens en heeft dus een grote verantwoordelijkheid om deze bijzondere persoonsgegevens goed te beschermen.

De Autoriteit Persoongegevens (AP) houdt toezicht op de naleving van de AVG. De AP kan flinke boetes uitdelen als een medewerker van een organisatie de regels niet volgt en daarmee de privacy van haar cliënten of medewerkers schendt. Ben je met persoonsgegevens bewust dat het om privacygevoelige informatie gaat.

Tip 1:



Print alleen persoonsgegevens als het echt nodig is. En vernietig ze na gebruik.

VRAAG JEZELF AF OF HET NODIG IS OM PERSOONSGEGEVENS TE PRINTEN.

Soms ontkom je er niet aan om documenten te printen. Maar je overtreedt de wet wanneer iemand anders vervolgens onbedoeld dat document in handen krijgt met daarop bijvoorbeeld persoonsgegevens of andere privacygevoelige informatie.

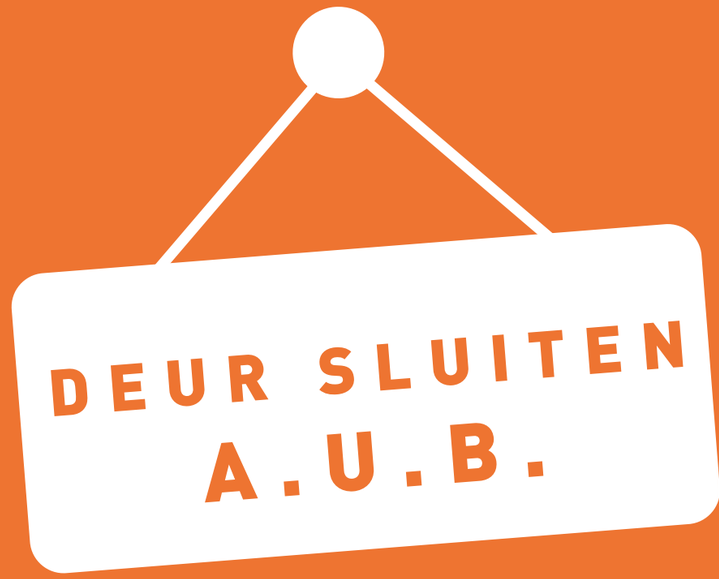
Vraag jezelf, in het kader van de privacy, daarom altijd af of het écht nodig is om gegevens te printen. Wanneer je privacygevoelige gegevens print, stop je ze na gebruik in de container voor vertrouwelijk papier (Platanenlaan 28 / Honk 1) of je vernietigt ze in een papierversnipperaar.

AVG
RECHTEN EN PLICHTEN

De kern van de AVG is dat persoonsgegevens niet in handen mogen komen van mensen, die niets met die gegevens van doen hebben. Ze zouden er misbruik van kunnen maken. Daarom zijn de rechten en plichten voor het verwerken van persoonsgegevens uitgebreid.

- Met de nieuwe wetgeving hebben betrokkenen, zoals cliënten, medewerkers en vrijwilligers meer rechten. Zo is het recht op inzage, het recht op informatie en het recht op wissen van gegevens uitgebreid.
- Organisaties hebben meer verplichtingen. Zo moet Severinus gedetailleerd vastleggen welke persoonsgegevens we verwerken en hoe we met de persoonsgegevens omgaan. Daarnaast moet Severinus ook een functionaris gegevensbescherming hebben, die adviseert over en toezicht houdt op de naleving van de AVG binnen de organisatie. Wie de functionaris binnen Severinus is, vind je op het intranet.

Tip 2:



Sluit de deur om te voorkomen dat er iemand onbedoeld meeluistert.

HOUD OVERLEG IN EEN RUIMTE WAAR PRIVACY IS GEBORGD.
In de zorg gaat het in een overleg vaak over cliënten en dus om privacygevoelige informatie. Om te voorkomen dat buitenstaanders deze informatie opvangen, is het van belang dat je bijvoorbeeld in een afgesloten ruimte zit, zeker tijdens een cliëntoverleg.

TOESTEMMING
OM PERSOONSGEGEVENS TE VERWERKEN

Volgens de AVG mogen medewerkers van Severinus persoonsgegevens van cliënten verwerken. Zij hebben deze gegevens nodig om zorg te kunnen verlenen. We hebben hiervoor een zorgovereenkomst met de cliënt. Severinus mag ook persoonsgegevens van medewerkers verwerken. Die zijn nodig om haar werkgeversrol uit te oefenen. Welke gegevens dit zijn, vind je in het privacyreglement (via de zoekfunctie van het intranet).

Wanneer persoonsgegevens niet direct te maken hebben met de zorg aan cliënten of de werkgeversrol van Severinus, moet je eerst toestemming vragen aan de betreffende cliënt of medewerker voordat je er iets mee kunt doen. Dit geldt bijvoorbeeld wanneer je persoonsgegevens wilt gebruiken voor huisbladen of een gedeelde digitale omgeving.

Vraag om toestemming

Tip 3:

We mogen alleen cliënt-persoonsgegevens gebruiken die we nodig hebben om zorg te verlenen of om de werkgeversrol uit te oefenen.

SOCIALE MEDIA

HET GEBRUIK VAN MEDEWERKER- EN CLIËNTGEGEVENS IN SOCIALE MEDIA

Sociale media, zoals WhatsApp, Facebook, Twitter, Instagram en Snapchat, gebruik je **niet** om informatie over cliënten en medewerkers te delen.

Zonder toestemming mág je zelfs geen foto's plaatsen op sociale media. Wil je toch graag een foto van een persoon via deze kanalen delen? Vraag dan altijd eerst vooraf schriftelijke toestemming aan de persoon. De persoon kan die toestemming ook weer intrekken. Je moet de foto dan weer verwijderen. Het toestemmingsformulier voor cliënten kun je vinden in het ECD (Elektronisch Cliëntendossier) of neem ervoor contact op met het Zorgbureau. Ook voor medewerkers checkt Severinus de toestemming altijd, dit loopt via de afdeling Communicatie & PR.

Tip 4:

Voor het delen van een foto van iemand op sociale media is toestemming nodig.

VEILIG INLOGGEN
HOE DOE JE DAT?

Wanneer je hetzelfde wachtwoord gebruikt voor meerdere websites, is dat hetzelfde als dezelfde sleutel gebruiken voor ieder slot. Wanneer iemand de sleutel in handen krijgt, kan hij overal binnen.

Wanneer een hacker jouw wachtwoord van een website heeft, kijkt hij vaak of het wachtwoord ook op andere websites te gebruiken is. Als je overal hetzelfde wachtwoord hanteert, zou hij zo ook toegang kunnen krijgen tot privacygevoelige gegevens. Het is daarom van belang om verschillende wachtwoorden voor je accounts te gebruiken.

Zorg ook voor een sterk wachtwoord. Hoe langer een wachtwoord is, hoe veiliger het is. Een goed wachtwoord bevat bovendien hoofdletters, kleine letters, leestekens en cijfers. Sommige websites vragen bij het inloggen, naast je wachtwoord, ook om een code. Daarmee wordt de beveiliging sterker. Wees dan ook alert met de Single-Sign-On mogelijkheid. Als je de computer bij verlaten van de ruimte niet goed afsluit, kan een onbevoegde eenvoudig toegang krijgen tot al jouw gegevens!

******

Tip 5:

Maak het hackers niet te makkelijk, gebruik verschillende en sterke wachtwoorden om in te loggen.

BEVEILIGD E-MAILEN
HOE DOE JE DAT?

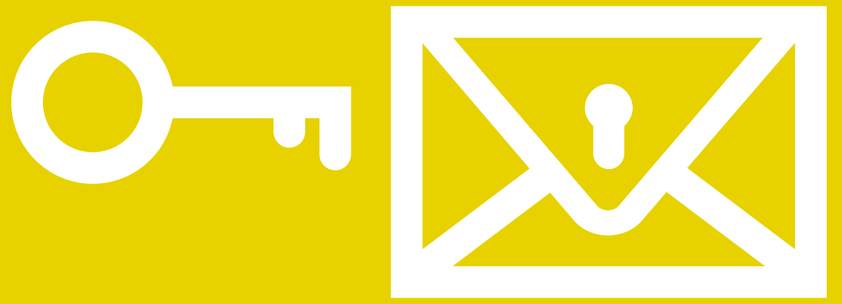
Om de privacy van medewerkers en cliënten te beschermen, kan het soms noodzakelijk zijn om je e-mails beveiligd te versturen. Bijvoorbeeld omdat je vertrouwelijke, medische en/of persoonsgegevens met de e-mail wilt versturen.

Beveiligd e-mailen is mogelijk met Zivver via Outlook. Zivver checkt automatisch je e-mail op medische termen, BSN-nummers en IBAN-nummers. Komt één van deze gegevens voor in je e-mail, dan wordt je e-mail automatisch versleuteld. Je krijgt daar vervolgens een melding van.

Als je e-mail niet automatisch wordt versleuteld, maar je het bericht toch beveiligd wilt versturen, geef dan bij het versturen aan dat je je e-mail wilt versleutelen.

Werkt de ontvanger ook met Zivver, dan kan hij het bericht lezen zonder dat hij daar extra handelingen voor hoeft te verrichten. Werkt de ontvanger niet met Zivver, dan krijgt hij een code of link waarmee hij het bericht kan openen.

Tip 6:



**Verstuur je persoonsgegevens met de e-mail?
Doe dat dan altijd versleuteld**

DATALEK
WAT TE DOEN?

Wanneer er per ongeluk of opzettelijk persoonsgegevens vrijgegeven worden aan anderen, die daar geen recht op hebben, noem je dat een datalek.

Denk je dat er sprake is van een datalek? E-mail dit dan direct aan het Privacy Informatieteam (PIT) van Severinus: **privacy@severinus.nl**. Het PIT beoordeelt of het datalek gemeld moet worden aan de Autoriteit Persoonsgegevens (AP). Als het datalek grote gevolgen heeft voor de cliënt(en) en/of medewerker(s), wordt dit ook aan hen gemeld. Zij kunnen dan maatregelen nemen. Het PIT probeert de gevolgen van het datalek zoveel mogelijk te beperken.

Wanneer je wegloopt van je computer, al is het maar om bijvoorbeeld een kopje koffie te halen, dan kan iedereen, bedoeld of onbedoeld, op je scherm gegevens zien of raadplegen. Dit is ook al een datalek! Ook is, in het geval van misbruik, achteraf niet meer te achterhalen of jij of iemand anders achter de computer heeft gezeten. Maak er daarom een gewoonte van om je scherm te vergrendelen zodra je wegloopt van je computer, **ook al ben je maar even weg**. Vergrendelen doe je eenvoudig door linksonder op vergrendelen te klikken of door de ctrl-alt-delete en entertoets in te drukken.

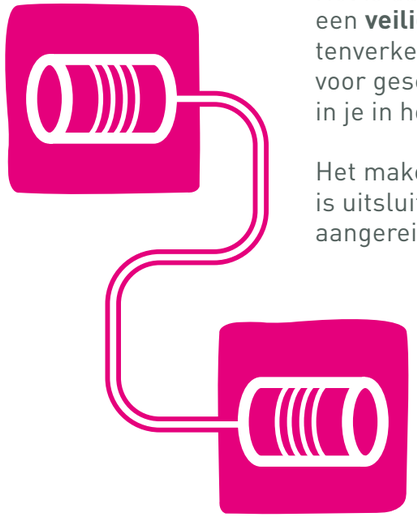
Tip 7:

Laat je computerscherm nooit onbeheerd open staan en vergrendel het scherm.

OMGAAN
MET CLIËNT- EN MEDEWERKERGEGEVENS

De cliëntgegevens houd je bij in het ECD en de medewerkergegevens staan in de HR-applicatie. Deze systemen zijn goed beveiligd.

In de praktijk wordt weleens gebruikgemaakt van een groepsapp of privé e-mail om te overleggen of om elkaar te informeren over cliënten. Dit is volgens de AVG niet toegestaan. Bij verschillende (gratis) berichtenapps of sociale media is het bovendien vaak onbekend of deze de privacyrichtlijnen naleven. Er is daarmee te veel onduidelijkheid over wat er met alle gesprekken en daarmee de gedeelde cliënt- en medewerkergegevens wordt gedaan.



Het is daarom van belang dat je samen met je team een **veilige communicatietool** gebruikt. Het berichtenverkeer in de communities op intranet zijn hiervoor geschikt. En clientgevoelige gegevens verwerk in je in het ECD.

Het maken en delen van beeldmateriaal van cliënten is uitsluitend toegestaan op door Severinus hiervoor aangereikte beveiligde apparatuur.

Tip 8:

ECD

Gebruik veilige middelen om te overleggen over cliënten en medewerkers.

TIEN TIPS!

1. Print alleen gegevens van een cliënt of medewerker als het echt nodig is. Bewaar deze persoonsgegevens nooit in een ruimte waar iedereen bij kan. Vernietig de prints na gebruik.

2. Praat nooit over cliënten en medewerkers in een openbare ruimte. Ga naar een afgesloten ruimte. Dan blijft het gesprek vertrouwelijk.

3. Ga na of je toestemming aan de cliënt of medewerker moet vragen om hun persoonsgegevens te verwerken.

4. Gebruik geen sociale media (Facebook, Whatsapp, Instagram enz.) om informatie over je werk en/of cliënten te delen. Maar gebruik veilige tools, zoals de community op het intranet of het ECD.

5. Gebruik verschillende en sterke wachtwoorden om in te loggen. Deel je wachtwoorden nooit met anderen.

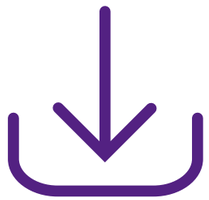
6. Laat je computerscherm nooit onbeheerd open staan, maar vergrendel je scherm altijd als je van je werkplek wegloopt (ctrl-alt-delete-enter).

7. Wil je persoonsgegevens e-mailen, doe dit dan altijd met een beveiligde e-mail. En controleer goed of je de e-mail naar de juiste persoon stuurt.

8. Denk je een datalek te herkennen, geef dit dan direct door aan het Privacy Informatieteam (PIT): **privacy@severinus.nl**.

9. Lees het privacyreglement goed door, zodat je vragen van cliënten en medewerkers kunt beantwoorden.

10. Houd intranet in de gaten. Daar worden artikelen geplaatst over de privacy. Wil je meer weten over privacy? Stel dan je vraag aan het PIT via **privacy@severinus.nl**.



PRIVACYBELEID, PRIVACYREGLEMENT EN PRIVACYVERKLARING

Op het intranet vind je het Privacybeleid en Privacyreglement van Severinus. In deze documenten geeft Severinus informatie over het verwerken van persoonsgegevens, de beveiliging daarvan en de rechten van betrokkenen. Daarnaast tref je op de website van Severinus de Privacyverklaring aan.

Lees de documenten goed door en wijs collega's er ook op. Zo ben je op de hoogte en kun je veilig handelen.

NOTITIES

SEVERINUS

BIJZONDER IN SAMENLEVEN