PRIVACYBELEID

Privacybeleid Severinus
Het privacybeleid van Severinus vormt het kader waarin wordt aangegeven op welke wijze Severinus omgaat met persoonsgegevens.

Het privacybeleid van Severinus is opgesteld, wordt uitgevoerd en gehandhaafd op basis van onder andere de volgende wettelijke kaders:
- *De Algemene Verordening Gegevensbescherming (AVG)*
- *Het Medisch Beroepsgeheim*
- *De Wet Cliëntenrechten bij Elektronische Verwerking van Gegevens*

Binnen Severinus worden persoonsgegevens verwerkt van betrokkenen: cliënten, medewerkers en derden. Een persoonsgegeven is elk gegeven is over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Het kan hierbij gaan om schriftelijke informatie, maar ook beeldmateriaal of bijvoorbeeld vingerafdrukken.

Severinus is zich bewust van de vertrouwelijkheid van persoonsgegevens en zorgt dat de privacy gewaarborgd blijft, dit door onder andere maatregelen te treffen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en verwerkerscontrole. Bovenal wil zij haar verwerkers van persoonsgegevens sturen op bewustwording.

De Directeur/Bestuurder en het Management spelen een cruciale rol bij het waarborgen van privacy, zij zijn eindverantwoordelijk. Het privacybeleid van Severinus is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en persoonsgegevensverzamelingen. Het beleid wordt iedere 2 jaar geëvalueerd en indien nodig herzien.

Grondslagen voor verwerkingen
Severinus gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. Severinus houdt zich hierbij aan de volgende uitgangspunten:

Rechtmatigheid, behoorlijkheid, transparantie
Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.

Grondslag en doelbinding
Severinus zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. De gerechtvaardigde doelen van Severinus zijn:
- Een optimale zorgverlening
- Goed werkgeverschap
- Het goed uitvoeren van wettelijke taken en verplichtingen

Dataminimalisatie
Severinus verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. Severinus streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

Bewaartermijn
Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om de zorgvragen en werkgever taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven.

Integriteit en vertrouwelijkheid
Severinus gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door benoemde personen en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt en stuurt Severinus voor passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in het **verwerkingsregister**.

Delen met derden
In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, stelt Severinus een overeenkomst op met eisen waar gegevensuitwisseling aan moet voldoen.

Subsidiariteit en Proportionaliteit
Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokkene zoveel mogelijk beperkt. Daarnaast mag de inbreuk op de belangen van de betrokkene niet onevenredig zijn in verhouding tot en met de verwerking te dienen doel.

Rechten van betrokkenen
Severinus informeert betrokkenen en honoreert (indien van toepassing) al hun rechten.

Algemene maatregelen
Severinus verwerkt algemene, gevoelige, bijzondere en (in uitzonderlijke gevallen) strafrechtelijke persoonsgegevens. Dit vraagt om organisatorische en installatietechnische veiligheidsmaatregelen.

Bewustwording
Severinus zorgt ervoor dat cliënten, medewerkers, vrijwilligers en derden betrokken bij de organisatie op de hoogte zijn van de (nieuwe) AVG regels. Veiligheid van persoonsgegevens moet verwerkt zijn in scholing, instructies en werkprocessen. Daarnaast moet aandacht voor veiligheid van persoonsgegevens/privacy zichtbaar aanwezig zijn in de organisatie.

Veiligheid van persoonsgegevens komt inhoudelijk binnen Severinus terug in:

- Het scholingsprogramma voor cliënten en medewerkers
- (in- en externe) Verwerkersovereenkomsten
- Het inwerkprogramma van medewerkers en vrijwilligers
- Het interne audit programma
- De algemene gedragscode/huisregels
- Interne/externe overlegstructuren
- Diverse mediakanalen (informatief)

Met als doel alle betrokkenen bij de verwerking van persoonsgegevens die competenties mee te geven dat zij kunnen inschatten: *het belang van de veiligheid van persoonsgegevens en wat de impact van de AVG is op uw huidige werkprocessen, diensten en goederen en welke conformaties en aanpassingen nodig zijn om aan de AVG te voldoen.*

Rechten van betrokkenen
De AVG geeft betrokkenen (de mensen van wie persoonsgegevens worden verwerkt) meer en verbeterde privacy rechten. Het gaat hierbij om bestaande rechten, zoals het recht op inzage en het recht op correctie en verwijdering, maar ook om nieuwe rechten, zoals het recht op data-portabiliteit.

Severinus wil betrokkenen informeren over de wijze waarop en waarvoor Severinus persoonsgegevens verwerkt en hun hierbij horende privacy rechten. Bovenal wil Severinus kenbaar maken dat zij alleen die persoonsgegevens verwerkt waarvoor zij (aantoonbaar) toestemming heeft gekregen van de betrokkenen. En dat het voor hen (bijvoorbeeld wanneer zij zich niet kunnen vereenzelvigen met het doel van de verwerking) mogelijk is om de toestemming in te trekken.

Severinus kent hiervoor:

- Een privacyreglement (incl. toestemmingsformulier beeldmateriaal) voor al haar (nieuwe) cliënten, medewerkers en vrijwilligers.
- Een privacyverklaring op haar intranet en website pagina.
- Een meldpunt voor betrokkenen: privacy@severinus.nl

Verwerkingsregister
Severinus kent een verwerkingsregister. In dit levende register staat vermeld:

- Welke persoonsgegevens worden verwerkt;
- het doel en wijze van de verwerking;
- wie de betrokkenen zijn (waar deze gegevens vandaan komen);
- met wie de gegevens worden gedeeld;
- de bewaartermijnen van de gegevens;
- de getroffen veiligheidsmaatregelen;
- en wie de verwerkingsverantwoordelijke is/verwerkers zijn.

Severinus eist dat haar verwerkingsverantwoordelijke (-n), (sub-) verwerkers en ontvangers zich conformeren aan de AVG en het privacybeleid van Severinus. Bovenal stelt zij dat binnen Severinus persoonsgegevens alleen verwerkt voor de beschreven doelen en alleen met de aan hen hiervoor (door Severinus) beschikbaar gestelde apparatuur, materialen, faciliteiten en voorzieningen.

Data protection impact assessment (DPIA)
Het DPIA is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen. Zodat tijdig maatregelen getroffen kunnen worden om eventuele risico's te verkleinen.

Severinus kent een eigen format DPIA en zal deze inzetten daar waar een beoogde gegevensverwerking een verhoogd privacy risico met zich meebrengt. Indien een verwerking noodzakelijk is voor de zorg-/bedrijf continuïteit, maar de DPIA een verhoogd risico uitwijst en het is niet mogelijk om maatregelen te vinden om dit risico te beperken, zal de verwerkingsverantwoordelijke dit proactief aan de Autoriteit Persoonsgegevens ter beoordeling voorleggen.

Privacy by design & privacy by default
Daar het niet altijd gaat om een verwerking met een hoog risico (waarbij een DPIA wordt afgenomen), stelt Severinus dat vooraf aan iedere verwerking (wel dan niet geautomatiseerd) bekend is:

- waarvoor (en welke) gegevens moeten worden verzameld (het gerechtvaardigd en noodzakelijk doel)
- wie de verwerkingsverantwoordelijke is

De verwerkingsverantwoordelijke bepaalt vervolgens wie verwerkers en ontvangers zijn, of een data protection impact assessment (DPIA) noodzakelijk is, op welke wijze betrokkenen en verwerkers worden geïnformeerd en of:

- Er gebruik gemaakt kan worden van bestaande veiligheidsvoorzieningen, protocollen en inrichtingen (privacy by design).
- Er nieuwe maatregelen dienen te worden getroffen om ervoor te zorgen dat, alléén persoonsgegevens veilig worden verwerkt noodzakelijk voor het specifieke doel (privacy by default).

De verwerkingsverantwoordelijke laat zich hierbij ondersteunen door het privacy informatie team (PIT) van Severinus en overige interne/externe deskundige disciplines. Deze uitwerking dient vooraf aan de verwerking door de verwerkingsverantwoordelijke (directeur/bestuurder) te worden beoordeelt en gekeurd. En indien goedgekeurd te worden opgenomen in het verwerkingsregister.

Verwerkersovereenkomsten
Severinus kent voor haar verwerkingen een interne verwerkersbeleid waarin de voorwaarden voor het verwerken van persoonsgegevens binnen Severinus staan benoemd. Deze verwerkersovereenkomst wordt aan iedere verwerker van persoonsgegevens binnen Severinus uitgereikt.

Daar waar Severinus de gegevensverwerking heeft uitbesteed aan een externe verwerker, zal de verwerkingsverantwoordelijke van Severinus zo veel als mogelijk het (naar Severinus vertaalde) model verwerkersovereenkomst van de brancheorganisaties zorg hanteren. Verwerkersovereenkomsten worden opgesteld en beoordeeld onder auspiciën van de Privacy Coördinator en worden beheert door de afdeling inkoop van Severinus.

Toezicht
Severinus kent een privacy informatie team (PIT). Het team bestaat uit de privacy coördinator, het hoofd informatieveiligheid en de functionaris voor de gegevensbescherming. Zij laten zich hierin bijstaan door een communicatie- en strategisch inkoopadviseur. Het PIT heeft als taak om:

- De bepalingen uit de AVG te vertalen naar Severinus;
- te adviseren (gevraagd en ongevraagd) en het houden van toezicht op bestaande, aangepaste of nieuwe verwerkingen binnen Severinus;
- DPIA's en verwerkersovereenkomsten te beoordelen;
- te fungeren als meldpunt voor aanvragen rond rechten van betrokkenen;
- het analyseren, beoordelen en indien noodzakelijk melden van datalekken.

Meldplicht datalekken
Wanneer zich een beveiligingsincident heeft voorgedaan waarbij persoonsgegevens verloren zijn gegaan, of wanneer onrechtmatige verwerking van persoonsgegevens niet redelijkerwijs kan worden uitgesloten, spreekt men van een datalek. Binnen Severinus kunnen datalekken (zowel door interne als externe personen/verwerkers) 24 uur per dag gemeld worden aan het PIT, de functionaris voor de gegevensbescherming (FG) of de consignatie (achter-) dienst van Severinus. Dit kan per mail (privacy@severinus.nl), via het incidenten meldsysteem (Itask) van Severinus of per telefonisch consult. Severinus verwijst betrokkenen, verwerkers en derden naar de informatie hieromtrent in haar protocollen, overeenkomsten en instructies.

Indien het PIT, de FG of Achterdienst op de hoogte raakt van een incident dat mogelijk onder de meldplicht datalekken valt, zal Severinus het incident onderzoeken en niet later dan 72 uur na de ontdekking een melding doen bij de Autoriteit Persoonsgegevens. Tenzij op dat moment uit het onderzoek is gebleken dat het incident niet onder de meldplicht datalekken valt. Hiervoor kent Severinus een format “onderzoek datalek”.

Ieder incident omtrent een datalek (of dit wel dan niet heeft geleid tot een melding) zal intern door het PIT geregistreerd en gedocumenteerd worden.