Security Statement Keerpunt

Informatiebeveiliging bij Keerpunt

Informatiebeveiliging is voor Keerpunt van cruciaal belang om de rechten en privacy van alle belanghebbenden te waarborgen. De essentie daarbij is de vertrouwelijkheid van deze gegevens (alleen toegankelijk voor de daartoe bevoegde personen), de beschikbaarheid van de gegevens (het voorhanden zijn van de informatie op het moment dat het nodig is) en de integriteit (juistheid en volledigheid). Om dit te borgen, heeft Keerpunt zowel organisatorisch als technisch passende beveiligingsmaatregelen genomen die in een continu proces op hun effectiviteit worden beoordeeld. Dit document geeft een overzicht van maatregelen die Keerpunt heeft ingeregeld.

Organisatorische beveiligingsmaatregelen

Certificeringen binnen Keerpunt

Keerpunt is in het bezit van het ISO certificaat **9001-2015 en het 'Certificaat Arbodiensten'.**
Het ISO certificaat wordt verstrekt als de dienstverlening voldoet aan de eisen conform de ISO 9001:2015 richtlijnen en de werkveld specifieke eisen uit de regeling van het certificatieschema. Deze eisen zijn vastgelegd in de Nederlandse Norm NEN-EN-ISO 9001:2015 + C1 en de regeling van de Minister van Sociale Zaken en Werkgelegenheid (Publicatie Staatscourant 29-11-2012).
Het 'Certificaat Arbodiensten' wordt verstrekt als de arbodienst voldoet aan verschillende eisen om haar deskundigheid te garanderen. Deze eisen zijn vastgelegd in de Arbowet, het Arbobesluit en de Arboregeling.
Keerpunt is aangesloten bij de OVAL, de brancheorganisatie van arbodiensten, interventiebedrijven, adviesbureaus op het terrein van outplacement en loopbaanbegeleiding en loopbaancoaching, re-integratiebedrijven en jobcoachorganisaties.

Privacyreglement

In ons privacyreglement staat precies omschreven welke gegevens wij verwerken, voor welke doeleinden wij gegevens verwerken, wie welke gegevens mag inzien, waar en hoe lang de gegevens bewaard worden, aan wie en op welke wijze wij de gegevens door kunnen geven en hoe we voorkomen dat onbevoegde personen de gegevens kunnen bekijken. Het privacyreglement is te vinden op onze website https://www.keerpunt.nl/privacy/.

Interne borging

Om de kwaliteit van onze dienstverlening continu te waarborgen, worden onze professionals (intern) opgeleid gericht op algemene vaardigheden voor het uitvoeren van de dienstverlening, maar ook met betrekking tot het naleven van de wet- en regelgeving.
Alle medewerkers van Keerpunt werken volgens de gedragscode van Keerpunt en hebben een geheimhoudingsverklaring ondertekend. Tevens wordt van nieuwe medewerkers altijd een VOG gevraagd voor indiensttreding.
Keerpunt heeft aansluitend een compliance awareness programma voor alle medewerkers waarin aandacht is voor onder andere privacyregelgeving.

Kwaliteitsmanagementsysteem

De werkprocedures binnen Keerpunt worden voortdurend getoetst aan de privacy-eisen uit de Algemene Verordening Gegevensbescherming, en de richtlijnen van de Autoriteit Persoonsgegevens. Zowel het privacyreglement als de werkprocedures zijn geïntegreerd in het door Keerpunt ontwikkelde Kwaliteitsmanagementsysteem. Deze aanpak zorgt niet alleen voor optimale beveiliging van de informatie, maar borgt door het cyclisch proces ook de continuïteit ervan voor de toekomst. Dat wij zulke hoge eisen stellen aan de privacy en de beveiliging van de persoons- en privacygevoelige gegevens, betekent dat wij ook hoge eisen stellen aan onze interne processen en

medewerkers. Onze medewerkers zijn zich bewust van de verantwoordelijkheid die zij hierin hebben. Jaarlijks toetsen we processen en werkwijzen binnen onze organisatie door middel van interne en externe audits waaronder inhoudelijke screening van de dossiers.
Daarnaast wordt als onderdeel van de reguliere jaarcontrole door onze accountant, specifiek een beoordeling uitgevoerd op de beveiliging van onze ICT-systemen. Elk jaar wordt aanvullend een zogenaamde penetratietest uitgevoerd door een daarin gespecialiseerd bedrijf om te beoordelen of het ICT landschap voldoet aan de huidige eisen.

Toegangsbeveiliging
Toegang tot Keerpunt kantoorruimtes is voorbehouden aan medewerkers en geregistreerde bezoekers.
Toegangsverlening tot, en binnen, de Keerpunt kantoorruimtes is enkel mogelijk middels een persoonsgebonden rfid-sleutel (fysieke toegangsprocedure).
Bezoekers worden in ruimtes waarin met gevoelige informatie wordt gewerkt, altijd begeleid door een Keerpunt medewerker.

Leveranciers
Met betrekking tot leveranciers waarvan wij diensten afnemen waar gegevensuitwisseling plaatsvindt en/of waar gebruik gemaakt wordt van applicaties ter ondersteuning van het primaire proces eisen wij van deze leveranciers dat zij beschikken over de relevante certificering zoals bijvoorbeeld ISO27001 of ISAE3402.

Incidentenprocedure
Keerpunt heeft een schriftelijk vastgelegde incidentenprocedure voor het classificeren, oplossen, en periodiek evalueren van incidenten. Zowel de IT- als de gebruikersorganisatie zijn ermee bekend dat incidenten volgens deze procedure worden opgelost.
De procedure datalekken wordt jaarlijks getoetst of deze voldoet aan de wet- en regelgeving.

Privacy Officer
Keerpunt heeft een Privacy Officer aangesteld en een Functionaris Gegevensbescherming (fg@keerpunt.nl) benoemd. Ontwikkelingen worden op de voet gevolgd en geïmplementeerd om continue compliance aan actuele privacy richtlijnen en wetgeving na te streven.

Technische beveiligingsmaatregelen
Keerpunt heeft in de automatisering diverse maatregelen genomen voor een optimale bescherming van (persoons)gegevens. Deze maatregelen worden middels interne audits getoetst.:

- De ICT-omgeving van Keerpunt is geplaatst in een veilige datacenter omgeving (ISO 27001 gecertificeerd).
- De toegang tot de ICT-omgeving gaat via secure verbindingen. De gegevens die op deze wijze over internet worden verstuurd, zijn op niveau beveiligd en versleuteld.
- Keerpunt maakt gebruik van een back-up systeem, waarbij alle gegevens die in de webapplicaties worden gebruikt direct bij opslag in de database ook in de back-up worden opgenomen. Dit garandeert dat ook bij calamiteiten geen gegevens verloren gaan. De toegang tot de back-up is beveiligd middels wachtwoorden. Fysieke toegang is middels rfid sleutels geregeld.
- Keerpunt maakt gebruik van SSL certificaten ter beveiliging van websites, portals en applicaties. Hierdoor wordt afgedwongen dat gebruikers de functionaliteit alleen kunnen benaderen via ‘https’ en dat de verbinding beveiligd is.
- Keerpunt hanteert een actief wachtwoordbeleid.
- Keerpunt hanteert Role Based Access (gebruikers krijgen alleen toegang tot die data waar men toe geautoriseerd is op basis van functie).
- Systemen binnen de Keerpunt ICT-omgeving hebben diverse koppelingen met applicaties of systemen van ketenpartners, die niet binnen hetzelfde datacenter zijn opgesteld. Bij het inrichten van deze koppelingen met applicaties of systemen van de ketenpartners wordt standaard gewerkt met certificaten en/of VPN verbindingen. Er worden alleen gegevens uitgewisseld die

volgens huidige wet- en regelgeving met de samenwerkende (keten)partners uitgewisseld mogen worden.

- Met ketenpartners en samenwerkingspartijen zijn afspraken vastgelegd over onder andere de gewenste beveiligingsmaatregelen, bewaartermijnen, geheimhouding, toegang tot de gegevens, melden van datalekken en op welke manier Keerpunt toeziet op naleving van de gemaakte afspraken. Keerpunt verricht bijvoorbeeld audits bij onze artsennetwerken om toezicht te houden op de naleving van de gemaakte afspraken.
- Van samenwerkingspartners eisen wij dat de mail communicatie via een versleutelde verbinding gaat.