Beveiligingsmaatregelen

KRAAMZORGCOMPLEET

#	Onderwerp	Maatregel
1	Informatiebeveiliging- en privacybeleid	Er is een informatiebeveiligings- en privacybeleid dat voldoet aan de AVG en eventuele richtsnoeren van de Autoriteit Persoonsgegevens en aansluit op de standaarden voor informatiebeveiliging ISO 27001 en NEN 7510. Dit beleid is intern gecommuniceerd en concreet geïmplementeerd door middel van gedocumenteerde procedures.
2	Certificering	Er is een managementsysteem voor informatiebeveiliging (gecombineerd ISMS/DPMS). Dit managementsysteem is opgezet en ingericht conform de standaarden voor informatiebeveiliging ISO 27001 en NEN 7510. Het systeem is gecertificeerd door de onafhankelijke auditpartij BSI.
3	Access management	De principes van 'least privilege' en 'need-to-know' worden toegepast op personeel en toegestane Subverwerkers. Gebruikerstoegang wordt tijdig ingetrokken of gewijzigd bij enige verandering in de status van personeel, leveranciers, klanten, zakelijke partners of derden. Er wordt gebruik gemaakt van actuele en algemeen als veilig beschouwde vormen van versleuteling en encryptie ten behoeve van identificatie, authenticatie en autorisatie.
4	Personeel	Medewerkers worden geïnformeerd over hun verantwoordelijkheden m.b.t. privacy en informatiebeveiliging en er wordt erop toegezien dat zij hun verplichtingen nakomen. Medewerkers die toegang hebben tot patiëntgegevens zijn gebonden aan geheimhouding.
5	Contractmanagement (Sub)verwerkers	Met iedere toegestane (Sub)verwerker wordt een (sub)verwerkersovereenkomst gesloten, die de (Sub)verwerker contractueel verplicht tot nakoming van dezelfde verplichtingen in verband met de verwerking als in de verwerkersovereenkomst waar deze bijlage bij hoort.
6	Security incident & response	Er is een gedocumenteerd security incident response plan dat geschikt is om Datalekken te detecteren, op te lossen en te melden, in overeenstemming met de verplichtingen in deze verwerkersovereenkomst.
7	Vulnerability / patchmanagement	Er wordt periodiek beoordeeld of er kwetsbaarheden binnen de gebruikte applicaties, systemen en netwerken zijn. Patches en updates voor gevonden kwetsbaarheden worden doorgevoerd.

8	Netwerk- en systeembeveiliging	Er zijn maatregelen getroffen om malware en misbruik van het netwerk en de systemen tegen te gaan en te detecteren (zoals firewalls en antivirussoftware van betrouwbare leveranciers).
9	Fysieke toegangsbeveiliging	Er zijn passende maatregelen (zoals sloten, camera's, alarmsystemen) genomen om de ruimtes waarin de Persoonsgegevens kunnen worden verwerkt, te beveiligen tegen onbevoegde toegang.
10	Logging	Er vindt logging plaats waarmee inzicht wordt verkregen in welke gebruikers op welke momenten inloggen.
11	Locatie	Persoonsgegevens worden verwerkt binnen de grenzen van de Europese Unie.
12	Business continuity & disaster recovery	Er is beleid en er zijn procedures en processen geïmplementeerd om te waarborgen dat de geleverde Diensten of Producten en de verwerkte Persoonsgegevens beschikbaar blijven in geval van onvoorziene omstandigheden en rampen, dan wel zo snel mogelijk volledig worden hersteld.
13	Applicatieontwikkeling – beveiligingsprincipes	Er worden beveiligingsprincipes toegepast om informatiebeveiliging in applicatieontwikkeling te integreren.
14	Onafhankelijke controle	Externe audits, kwetsbaarheidsscans en penetratietests worden periodiek uitgevoerd op applicaties en netwerken om zwakheden en potentiële Datalekken te ontdekken.