BIJLAGE 5 DATAPROTOCOL LDF - PROTOCOL BEVEILIGINGSBEHEER

Dit protocol Beveiligingsbeheer heeft betrekking op de maatregelen die zijn en worden genomen in het kader van verlies of beschadiging van of ongeautoriseerde toegang tot persoonsgegevens, danwel overige incidenten ten aanzien van persoonsgegevens (een “incident”), en de stappen die ondernomen worden indien een incident zich voordoet.

Alle werknemers van Partijen worden geacht op de hoogte te zijn van en te handelen in lijn met dit protocol.

Aanspreekpunt
Iedere Partij heeft een medewerker aangesteld die als contactpersoon fungeert in het kader van het beveiligingsbeleid. Deze medewerker wordt als Security Officer aangeduid. De Security Officer is verantwoordelijk voor het aansturen en coördineren van de (uitvoering van) dit Protocol beveiligingsbeheer. In dat kader heeft de Security Officer onder meer de volgende taken:

- Fungeren als meldpunt voor incidenten;
- Het (doen) instellen van een onderzoek naar het incident, waaronder ten minste begrepen de omvang van het incident, de betrokken persoonsgegevens en de wijze van ontstaan van het incident;
- Het (doen) initiëren van een actieplan en/of disaster recovery plan
- MediQuest en/of IQ Healthcare: het doorgeven van het incident aan KNGF;
- KNGF: het beoordelen of het incident kwalificeert als een datalek in de zin van artikel 34a Wet bescherming persoonsgegevens en het melden van een incident bij de Autoriteit Persoonsgegevens;
- KNGF: het beoordelen – tezamen met de daarbij relevante personen binnen zijn/haar Partij, zoals bijvoorbeeld de juridische afdeling – of het datalek ook gemeld moet worden aan de betrokkene en zo ja, het (doen) verrichten van de melding aan de betrokkene;
- Het – in samenspraak met de daarbij relevante personen binnen zijn/haar Partij, zoals bijvoorbeeld de technische en/of juridische afdeling – (doen) treffen van maatregelen ter voorkoming en/of beperking van (de gevolgen van) het incident. MediQuest en/of IQ Healthcare zullen te treffen maatregelen altijd vooraf afspreken met KNGF;
- Het tijdig aanleveren van de in dit Protocol beveiligingsbeheer vermelde rapportages;
- Beantwoorden van vragen van medewerkers over informatiebeveiliging en toepassing van het Protocol beveiligingsbeheer;
- Het regelmatig reviewen van dit Protocol beveiligingsbeheer en waar nodig zorg dragen voor het bijstellen van dit protocol.

Incidenten
Indien een werknemer constateert of het redelijk vermoeden heeft dat er een incident heeft plaatsgevonden, zal hij/zij dit, vergezeld van zo veel mogelijk informatie omtrent het (vermoedelijke) incident, zo spoedig mogelijk melden aan zijn Security Officer. De Security Officer zal de melding van de werknemer beoordelen en de vereiste maatregelen treffen op de wijze als hiervoor weergegeven.

MediQuest en IQ Healthcare zullen (via hun Security Officer) de Security Officer van KNGF

zo spoedig mogelijk – doch uiterlijk binnen 24 uur – op de hoogte stellen van het incident op de door de KNGF opgegeven contactgegevens.

De melding aan de KNGF bevat, voor zover mogelijk, de volgende gegevens:

- een beschrijving van het incident, waaronder de aard, de datum/periode en de omvang van het incident, alsmede het type persoonsgegevens en het aantal betrokkenen waarvan de persoonsgegevens betrokken zijn bij het incident;
- de (mogelijke) gevolgen van het incident;
- de genomen of aanbevolen maatregelen om de gevolgen van het incident zo veel mogelijk te beperken;
- de verwachte tijd die gemoeid is met het oplossen van (de gevolgen van) het incident.

Voorts zal de Partij bij wie het incident zich heeft voorgedaan KNGF op de hoogte houden van de ontwikkelingen aangaande het incident en KNGF voorzien van regelmatige rapportages dienaangaande.

MediQuest en IQ Healthcare zullen in het kader van het incident aan alle redelijke verzoeken van KNGF voldoen en indien vereist hun medewerking verlenen. Waar mogelijk en/of vereist omvatten de maatregelen die Partijen treft in het kader van een incident work-arounds om onderliggende bedrijfsprocessen draaiende te houden tot de systemen volledig hersteld zijn.

Maatregelen en Standaarden

De door Partijen doorgevoerde beveiligingsmaatregelen zijn gespecificeerd in Bijlage 4 bij het Dataprotocol LDF.

Audit

Partijen zullen eenmaal per jaar een audit uitvoeren. Onderdeel van een dergelijke audit is ten minste het onderzoeken of de beveiligingsmaatregelen zoals bedoeld in Bijlage 4 daadwerkelijk zijn geïmplemteerd, of de beveiligingsmaatregelen en/of het beleid inzake deze beveiligingsmaatregelen zwakke plekken bevat en/of nog steeds passend is gezien de te verwerken gegevens en/of de stand van de techniek, alsmede om te toetsen of het informatiebeveiligingsbeleid binnen het bedrijf of de instantie voldoende wordt nageleefd. De resultaten van de audit zullen aan het management van die Partij, alsmede aan de andere Partijen bij het Dataprotocol LDF worden gerapporteerd.