PROTOCOL BEVEILIGINGSINCIDENTEN

Witte Kruis Transplant B.V. garandeert passende technische en organisatorische maatregelen om persoonsgegevens en rechten van betrokkenen te beschermen zijn conform de vereisten van de Algemene Verordening Gegevensbescherming (AVG). Ondanks deze passende beveiligingsmaatregelen is het mogelijk dat een beveiligingsincident ontstaat waarbij per ongeluk of op onrechtmatige wijze doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens mogelijk worden vernietigd, verloren, gewijzigd, ongeoorloofd verstrekt of ongeoorloofd toegang tot wordt verschaft.

Indien er sprake van een dergelijk beveiligingsincident zal de directie van Witte Kruis Transplant B.V. deze documenteren door middel van het formulier "Documentatie beveiligingsincidenten" (zie einde protocol). De directie van Witte Kruis Transplant B.V. zal maatregelen nemen die redelijkerwijs van haar kunnen worden verwacht om het incident zo snel mogelijk te herstellen dan wel de verdere gevolgen zoveel mogelijk te beperken.

Indien bij het beveiligingsincident partijen waarmee verwerkersovereenkomsten gesloten zijn (verwerkingsverantwoordelijken dan wel (sub-)verwerkers) betrokken zijn, zal de directie van Witte Kruis Transplant B.V. deze partijen zonder onredelijke vertraging informeren over het beveiligingsincident en in overleg treden met deze partijen om nadere afspraken te maken over te nemen maatregelen. Partijen waarmee verwerkingsovereenkomsten zijn gesloten worden tevens na een melding van een beveiligingsincident geïnformeerd over ontwikkelingen betreffende het beveiligingsincident.

Melding Autoriteit Persoonsgegevens
Indien bij het beveiligingsincident persoonsgegevens verloren zijn gegaan of onrechtmatige verwerking redelijkerwijs niet uit te sluiten is, is er sprake van een datalek. Indien er met dit datalek persoonsgegevens van gevoelige aard gemoeid zijn of er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, dient het datalek gerapporteerd te worden bij de Autoriteit Persoonsgegevens (AP). De directie van Witte Kruis Transplant B.V. meldt dergelijke beveiligingsincidenten direct dan wel binnen 72 uur na het beveiligingsincident via het online meldloket https://datalekken.autoriteitpersoonsgegevens.nl/.

Wanneer Witte Kruis Transplant B.V. in de hoedanigheid van verwerkingsverantwoordelijke verkeerd, is zij verantwoordelijk voor de melding bij de Autoriteit Persoonsgegevens. Dit geldt ook indien het beveiligingsincident is ontstaan bij een (sub-)verwerker of een (sub-)verwerker betrokken is bij het beveiligingsincident. Witte Kruis Transplant B.V. kan een beroep doen op de (sub-)verwerker om zoveel mogelijk te ondersteunen bij het verzamelen van informatie, het communiceren naar betrokkenen en het doen van de melding.

Wanneer Witte Kruis Transplant B.V. in de hoedanigheid van verwerker verkeerd, is zij niet verantwoordelijk voor de melding bij de Autoriteit persoonsgegevens. Zij zal in dat geval de verwerkingsverantwoordelijke zoveel mogelijk bijstaan bij het verzamelen van informatie, het communiceren naar betrokkenen en het doen van de melding.

Melding Betrokkenen
Indien bij het beveiligingsincident sprake is van een datalek welke gerapporteerd moet worden bij de AP én niet alle gelekte gegevens (goed) versleuteld waren of er (waarschijnlijk) sprake is van ongunstige gevolgen voor de persoonlijke levenssfeer van betrokkenen, is de directie van Witte Kruis Transplant B.V. verantwoordelijk om dit te melden aan de betrokkenen.

Documentatie beveiligingsincidenten

Aard	*Geef een beschrijving van het incident*
Oorzaak	*Geef aan wat de oorzaak van het incident was.*
Gevolgen	*Geef aan wat de geconstateerde en vermoedelijke gevolgen van het incident zijn.*
Duur	*Geef zo precies mogelijk aan op welke datum en tijd het incident begon en op welke datum en tijd het incident eindigde of geef aan in welke periode het incident plaatsvond.*
Categorieën getroffen Persoonsgegevens	*Geef aan welke categorieën Persoonsgegevens getroffen zijn, zoals NAW, e-mailadres, IP-nummer, BSN, etc.*
Categorieën getroffen Betrokkenen	*Geef aan welke categorieën Betrokkenen getroffen zijn, zoals medewerkers, sollicitanten, klanten, externe contacten, etc.*
Maatregelen (nu)	*Geef aan welke maatregelen de Verwerker heeft genomen of zal nemen om het incident in te perken en/of op te lossen.*
Maatregelen (toekomst)	*Geef aan welke maatregelen de Verwerker heeft genomen of zal nemen om dergelijke incidenten in de toekomst te voorkomen.*