Nadere afspraken omgang beveiligingsincident

Achtergrond

In de verwerkersovereenkomst nieuwe stijl zoals deze tot stand is gekomen met het oog op huidige wetgeving is vermeld dat nadere afspraken gemaakt worden over de nadere invulling en naleving van de Algemene Verordening Gegevensbescherming (AVG), meer in het bijzonder van de naleving van de meldplicht datalekken als de richtsnoeren van de Autoriteit Persoonsgegevens (AP) naar aanleiding van de meldplicht datalekken van kracht zijn geworden. Dat geldt zowel voor een beveiligingsincident bij de verwerkingsverantwoordelijke als bij de verwerker. Het doel is naast wederzijdse tijdige en juiste informatie-uitwisseling, het voorkomen van escalatie in brede zin des woords.

Dit document bevat een aantal afspraken maar is geen standaardprotocol dat iedere situatie volledig kan en zal afdekken. Gezond verstand en onderling overleg zullen altijd noodzakelijk blijven.

Basisaanpak

Contactgegevens

Om bij incidenten met persoonsgegevens snel en met de juiste personen contact op te kunnen nemen moeten vooraf de wederzijdse contactgegevens bekend zijn. Dit kunnen de contactgegevens van de Functionaris Gegevensbescherming (FG) zijn of de persoon die binnen de organisatie als contactpersoon voor beveiligingsincidenten benoemd is (beide hierna: contactpersoon). Deze contactpersoon zal bij incidenten de verdere communicatie binnen de eigen organisatie verzorgen en aanspreekpunt zijn voor de wederpartij.

Verwerkingsverantwoordelijke en verwerker zorgen er voor dat de contactpersonen voldoende gemandateerd zijn om dit overleg te voeren.

Voor doorgifte van de contactgegevens kan het formulier zoals opgenomen in bijlage 1 gebruikt worden. Op het moment dat de contactgegevens wijzigen zullen partijen elkaar onmiddellijk de betreffende wijzigingen doorgeven per e-mail via het formulier.

De actuele contactgegevens voor de privacy verantwoordelijke bij Nedap Healthcare staan vermeld op het Nedap Supportportaal onder het kopje: “Incidenten en datalekken”.

Melding van incidenten

Incidenten in de keten van verwerkingen kunnen zich op velerlei manieren voordoen. De volgende scenario’s zijn bijvoorbeeld denkbaar:

- Er is een beveiligingsincident bij de verwerkende partij. De verwerker informeert zonder onredelijke vertraging de getroffen verwerkingsverantwoordelijke middels een zo compleet mogelijk ingevuld meldingsformulier (zie bijlage 2), in ieder geval per e-mail en zo mogelijk ook aansluitend per telefoon. De verwerkingsverantwoordelijke bevestigt de goede ontvangst van het meldingsformulier.

- Er is een beveiligingsincident bij de verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke informeert zonder onredelijke vertraging de relevante/getroffen verwerker middels een zo compleet mogelijk ingevuld meldingsformulier (zie bijlage 2), in ieder geval per e-mail en zo mogelijk ook aansluitend per telefoon. De verwerker bevestigt de goede ontvangst van het meldingsformulier.

Nadat de melding is ontvangen vindt onderlinge afstemming plaats. Afhankelijk van de ernst van de situatie en de aard van het beveiligingsincident overleggen bovenbedoelde contactpersonen namens hun beider organisaties of:

- melding aan de AP gedaan dient te worden, en/of;
- melding aan de betrokkenen dient plaats te vinden;
- welke meldingstekst en informatie hiervoor gebruikt gaat worden. In geval eerst nader onderzoek noodzakelijk is, zullen de getroffen partijen overwegen of gezien het dwingende tijdschema een voorlopige melding gedaan zal worden;
- andere verantwoordelijken geïnformeerd dienen te worden;
- andere (sub)verwerkers geïnformeerd dienen te worden;
- aanvullend onderzoek door of op initiatief van verwerkingsverantwoordelijke bij verwerker ondernomen zal worden. Dit onderzoek staat apart van hetgeen in de verwerkersovereenkomst is bepaald. De kosten van het onderzoek komen voor rekening van de verwerkingsverantwoordelijke.

Naarmate de verwerker verder afstaat van de gegevens of het systeem dat getroffen is door een beveiligingsincident, zal deze zich meer terughoudend opstellen inzake de invulling en uitvoering van de hier genoemde actiepunten.

Voor de vastlegging van de documentatie behorende bij het beveiligingsincident wordt het formulier zoals bijgevoegd in bijlage 2 gebruikt. Het zal een iteratief proces zijn. Naarmate het onderzoek voortgaat komt er meer informatie beschikbaar waardoor de documentatie steeds completer wordt. Het is de bedoeling dat uiteindelijk alle onderdelen van het formulier ingevuld zijn door die partij waar het beveiligingsincident heeft plaatsgevonden en dat dit met alle betrokken partijen gedeeld is. Na de eerste melding zal telkens een update van de situatie via een aangepast formulier plaatsvinden op die momenten dat dit zinvol geacht wordt.

<u>Communicatiewijze</u>

Het verdient de voorkeur om te communiceren per telefoon. Het kan echter vanwege tijdstip of aantal contactpersonen de voorkeur verdienen eerst per e-mail te communiceren. Indien gecommuniceerd wordt per telefoon, bevestigen partijen achteraf schriftelijk de inhoud van het besprokene en de gemaakte afspraken.

Partijen nemen maatregelen om er voor te zorgen dat het opgegeven telefoonnummer en e-mailadres actueel is. Minimaal 1x per dag wordt gecontroleerd op binnengekomen e-mailberichten.

De mogelijkheid blijft bestaan dat toekomstige nieuwe manieren van communicatie toegevoegd worden.

Bijlage 1 - Formulier contactgegevens inzake beveiligingsincidenten

Organisatiegegevens:

Naam	
Adres	
Postcode	
Woonplaats	
Telefoonnummer	
Emailadres	

Contactgegevens contactpersoon:

Naam	
Adres	
Postcode	
Woonplaats	
Vaste telefoonnummer	
Mobiele telefoonnummer	
Faxnummer	
E-mailadres	
Functie/rol	

Bijlage 2 – Meldingsformulier datalek ketenpartner

Organisatienaam	

(Vermoedelijke) Datum en tijdstip datalek	
Datum en tijdstip constatering datalek	
Datum en tijdstip melding ketenpartner	

Wijze van constatering alsmede door wie geconstateerd

Omschrijving datalek

Geconstateerde gevolgen voor de gegevensverwerking

Getroffen gegevens (welke en aantallen)

Getroffen betrokkenen

Is het op basis van de beschikbare informatie noodzakelijk dat ook de betrokkenen worden ingelicht. Zo ja, welke informatie. Zo nee, wat is hiervoor de onderliggende motivatie.

Gekozen tijdelijke oplossing

Gekozen structurele oplossing

Verstuurde informatie extern

Waar informatie te verkrijgen

Aanbevolen maatregelen om nadelige gevolgen te beperken

Motivatie voor de gedane melding