Handreiking afhandelen van inbreuken in verband met persoonsgegevens GGD Zuid-Limburg

1. Inleiding

Met de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) is voor organisaties die persoonsgegevens verwerken de verplichting ingevoerd om een inbreuk in verband met persoonsgegevens te melden aan de nationale toezichthouder (hierna: Autoriteit Persoonsgegevens) en om in bepaalde gevallen de inbreuk ook mede te delen aan degenen waarvan persoonsgegevens betrokken zijn bij de inbreuk.
In aanvulling op de AVG, dient een zorgorganisatie als de GGD Zuid Limburg te voldoen aan de geldende normen voor informatiebeveiliging in de zorg, de NEN7510:2017. Deze norm is van toepassing op alle zorgaanbieders en organisaties in de zorg- en welzijnssector die persoonlijke gezondheidsinformatie beheren. Een van de norm-eisen legt de verplichting op aan zorgorganisaties om verantwoordelijkheden en procedures vast te stellen met betrekking tot het managen van beveiligingsincidenten.

Deze handreiking is opgesteld zodat inbreuken in verband met persoonsgegevens overeenkomstig het wettelijk- en normenkader van de AVG en de NEN7510:2017 worden opgevolgd en afgehandeld.

2. Wettelijk- en normenkader

De volgende wettelijke bepalingen en norm-eis(en) bepalen de kaders voor de afhandeling van inbreuken in verband met persoonsgegevens.

2.1. Algemene Verordening Gegevensbescherming (AVG)

1. Artikel 4 onder 12 van de AVG.
Dit artikel definieert een inbreuk in verband met persoonsgegevens als volgt:

een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Het gaat om een inbreuk op de beveiliging van persoonsgegevens, waardoor er ongeoorloofde of onbedoelde toegang tot persoonsgegevens heeft plaatsgevonden, of waardoor persoonsgegevens per ongeluk of op onrechtmatige wijze zijn verstrekt, vernietigd, gewijzigd of verloren gegaan.

2. Artikel 33 van de AVG
Dit artikel bepaalt dat indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, de verantwoordelijke organisatie deze inbreuk zonder onredelijke vertraging, doch uiterlijk binnen 72 uur na ontdekking, aan de Autoriteit Persoonsgegevens dient te melden, tenzij er waarschijnlijk geen risico op nadelige gevolgen voor de privacy van de betrokkenen bestaat.

3. Artikel 34 van de AVG
Dit artikel bepaalt dat indien er door de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico op nadelige gevolgen voor de privacy van de betrokkenen bestaat, de verantwoordelijke de betrokkene(n) onverwijld op de hoogte brengt van de inbreuk. Het

informeren van de betrokkene(n) kan achterwege blijven indien een van de volgende voorwaarden is vervuld:

a. De verantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk betrekking heeft, zoals versleuteling;
b. De verantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het hoge risico zich waarschijnlijk niet meer zal voordoen; of
c. De mededeling zou onevenredige inspanning vergen.

2.1.1. Beoordeling risico en hoog risico

Voor het beoordelen van het risico en hoog risico op nadelige gevolgen voor de privacy van de betrokkenen, wordt overeenkomstig de door de WP29 opgestelde Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 (p. 26 en verder) gehandeld. Er wordt bij het beoordelen van het risico en hoog risico rekening gehouden met in ieder geval de volgende criteria:

- De aard van de inbreuk (inbreuk op vertrouwelijkheid, integriteit of beschikbaarheid);
- De aard, omvang en gevoeligheid van de gelekte gegevens;
- Het aantal getroffen personen;
- Het gemak waarmee de personen waarvan gegevens zijn gelekt kunnen worden geïdentificeerd;
- De ernst van de gevolgen voor deze personen;
- De bijzondere kenmerken van deze personen (bv. kwetsbare groepen zoals kinderen);
- De bijzondere kenmerken van de organisatie.

Een *hoog risico* bestaat als de inbreuk kan leiden tot lichamelijke, materiële of immateriële schade voor de personen waarvan de gegevens betrokken zijn bij de inbreuk. Voorbeelden van dergelijke schade zijn discriminatie, identiteitsdiefstal of -fraude, financieel verlies en reputatieschade. Wanneer de inbreuk betrekking heeft op bijzondere persoonsgegevens, zoals gegevens over ras of etnische afkomst, politieke opvatting, religie of levensbeschouwelijke overtuigingen, vakbondslidmaatschap, gegevens over iemands gezondheid of seksleven, strafrechtelijke veroordelingen of strafbare feiten, moet dergelijke schade als waarschijnlijk worden beschouwd (Overweging 75 en 76 van de AVG).

2.2. NEN 7510:2017 – A.16.1.2. Rapportage van informatiebeveiligingsgebeurtenissen

Op basis van deze norm-eis dienen organisaties een cliënt altijd te informeren als er per ongeluk persoonlijke gezondheidsinformatie openbaar is gemaakt.

Het begrip 'persoonlijke gezondheidsinformatie' wordt als volgt gedefinieerd:

Informatie over een identificeerbare persoon die verband houdt met de lichamelijke of geestelijke gesteldheid van, of de verlening van zorgdiensten aan, de persoon in kwestie, waaronder ook begrepen kan worden:

- *informatie over de registratie van de persoon voor de verlening van zorgdiensten;*
- *informatie over betalingen of het in aanmerking komen voor zorg met betrekking tot de persoon;*
- *een aan een persoon toegewezen nummer, symbool of bijzonderheid als unieke identificatie van die persoon voor medische doeleinden;*
- *alle informatie over de persoon die wordt vergaard tijdens het verlenen van zorgdiensten aan de persoon;*
- *informatie die is ontleend aan een beproeving of onderzoek van een lichaamsdeel of lichaamseigen stof, en*

- *identificatie van een persoon (bijvoorbeeld een zorgprofessional) als verlener van zorg aan de persoon.*

Het begrip 'openbaar gemaakt' wordt in de NEN7510:2017 niet gedefinieerd. Binnen de GGD Zuid Limburg wordt derhalve 'openbaar gemaakt' als volgt gedefinieerd:

Persoonlijke gezondheidsinformatie wordt bekend gemaakt aan iemand zonder behandelrelatie en diegene is ook niet anderszins bij de behandeling van de cliënt betrokken.

3. Afhandelen van inbreuken in verband met persoonsgegevens

Om inbreuken in verband met persoonsgegevens overeenkomstig bovenstaand wettelijk- en normenkader van de AVG en NEN7510:2017 af te handelen, worden dergelijke inbreuken als volgt opgevolgd en afgehandeld.

3.1. Melden aan de Autoriteit Persoonsgegevens

Inbreuken in verband met persoonsgegevens worden conform artikel 33 van de AVG opgevolgd en afgehandeld. Dit houdt in dat er een beoordeling van het risico plaatsvindt op basis van de onder 2.1.1. opgenomen criteria. Indien er op basis van deze risicobeoordeling waarschijnlijk een risico op nadelige gevolgen voor de privacy van de betrokkenen bestaat, dan wordt de inbreuk gemeld aan de Autoriteit Persoonsgegevens. Concreet betekent dit dat de Functionaris Gegevensbescherming na bekend worden met de inbreuk een risicobeoordeling op basis van bovenstaande criteria zal uitvoeren. Bestaat er waarschijnlijk een risico op nadelige gevolgen voor de privacy van de betrokkenen, dan zal de Functionaris Gegevensbescherming de verantwoordelijke afdeling adviseren om de inbreuk te melden aan de Autoriteit Persoonsgegevens. De daadwerkelijke melding aan de Autoriteit Persoonsgegevens doet de Functionaris Gegevensbescherming.

3.2. Melden aan betrokkenen

3.2.1. Inbreuken waarbij persoonlijke gezondheidsinformatie openbaar wordt gemaakt

Bij inbreuken waarbij persoonlijke gezondheidsinformatie per ongeluk openbaar wordt gemaakt, wordt de norm-eis A.16.1.2. uit de NEN7510:2017 gevolgd. Inbreuken waarbij per ongeluk persoonlijke gezondheidsinformatie openbaar is gemaakt, worden altijd gemeld aan de betrokkenen. De verantwoordelijke afdeling meldt het openbaar maken van de persoonlijke gezondheidsinformatie aan de betrokkenen. Daarvoor is een standaard brief beschikbaar gesteld waarin informatie is opgenomen die minimaal aan de betrokkenen medegedeeld dient te worden.

3.2.2. Inbreuken met andere persoonsgegevens dan persoonlijke gezondheidsinformatie

Inbreuken waarbij andere persoonsgegevens zijn betrokken dan persoonlijke gezondheidsinformatie worden conform artikel 34 van de AVG opgevolgd en afgehandeld. Dit houdt in dat er een beoordeling van het hoog risico plaatsvindt op basis van de onder 2.1.1. opgenomen criteria. Indien er op basis van deze risicobeoordeling waarschijnlijk een hoog risico op nadelige gevolgen voor de privacy van de betrokkenen bestaat, dan wordt de inbreuk gemeld aan de betrokkenen. Concreet betekent dit dat de Functionaris Gegevensbescherming na bekend worden met de inbreuk een risicobeoordeling op basis van bovenstaande criteria zal uitvoeren. Bestaat er waarschijnlijk een hoog risico op nadelige gevolgen voor de privacy van de betrokkenen, dan zal de Functionaris Gegevensbescherming de verantwoordelijke afdeling adviseren om de inbreuk te melden aan de betrokkenen. De daadwerkelijke melding aan betrokkenen doet de verantwoordelijke afdeling. Daarvoor is een standaard brief beschikbaar gesteld waarin informatie is opgenomen die minimaal aan de betrokkenen medegedeeld dient te worden.