PROCEDURE DATALEKKEN

DE PSYCHOLOGENGROEP GGZ

1. Inhoud

2. Inleiding

Met ingang van 1 januari 2016 geldt volgens de Wet bescherming persoonsgegevens (Wbp) de meldplicht voor datalekken. Per 25 mei is deze verplichting via de Algemene verordening Gegevensbescherming onderdeel van Nederlandse wet- en regelgeving.

Volgens deze meldplicht moeten organisaties die persoonsgegevens verwerken, datalekken melden aan Autoriteit Persoonsgegevens (AP) (en in bepaalde gevallen ook aan de betrokkenen) als het leidt tot (of een aanzienlijke kans dat dit leidt tot) ernstige nadelige gevolgen in relatie tot de integriteit / bescherming van persoonsgegevens.
Een datalek treedt op wanneer er persoonsgegevens inzichtelijk worden voor ongeautoriseerde personen, of wanneer persoonsgegevens onbeschikbaar worden (dus, als een computer crasht met daarop persoonsgegevens en je hebt geen back-up).

Definitie 'Persoonsgegevens'
'alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene) (art.4, sub 1, AVG). Een persoon is identificeerbaar indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden. Er kan een onderscheid worden gemaakt in direct en indirect identificerende gegevens.
Direct identificerende gegevens zijn gegevens die betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig is vast te stellen, zoals een naam, evt. in combinatie met het adres en de geboortedatum.
Van indirect identificerende gegevens is sprake wanneer gegevens via nadere stappen in verband kunnen worden gebracht met een bepaalde persoon.
Een gegeven is geen persoonsgegeven, indien doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijk personen redelijkerwijs wordt uitgesloten'.

Definitie 'Verwerking'
Een bewerking of geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens (art.4 sub b, AVG)'.

De Psychologengroep heeft de plicht om iedere melding van een datalek te onderzoeken op ernst en impact. Als na onderzoek blijkt dat er sprake is van een datalek dat gemeld moet worden aan de AP, dan dient deze melding binnen 72 uur plaats te vinden.
Te denken valt aan:

- een kwijtgeraakte USB-stick
- een gestolen laptop
- een inbraak door een hacker
- verzending van e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden
- een malware-besmetting
- een calamiteit zoals een brand in een datacentrum
- gecrashte computer met persoonsgegevens en je hebt geen back-up

Verschil tussen een Beveiligingsincident en een Datalek
Een beveiligingsincident is een incident waarbij de beschikbaarheid, vertrouwelijkheid of integriteit van informatie gecompromitteerd wordt. (Een datalek is een voorbeeld van een beveiligingsincident).
Er is sprake van een beveiligingsincident als iemand ongeautoriseerde toegang heeft verkregen tot ruimte, systemen, informatie.
Bij een beveiligingsincident maakt de directie de afweging of er sprake kan zijn van een datalek en of deze gemeld moet worden bij de Autoriteit Persoonsgegevens.

Definitie 'Betrokkenen'
'Is/zijn degene(n) van wie persoonsgegevens zijn gelekt'.

Een datalek moet naast aan de AP ook aan de betrokkene(n) worden gemeld als het datalek waarschijnlijk ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkenen. (Achterliggende gedachte hierbij is dat betrokkenen in een zo vroeg mogelijk stadium in staat gesteld worden maatregelen te nemen teneinde de impact van het datalek op hun persoonlijke levenssfeer te beperken).

Definitie 'Verwerkers'
Natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. (artikel 4, sub 8, AVG)'.

Ook een verwerker is drager van rechten en plichten en dient niet alleen de instructies van de verantwoordelijke op te volgen maar is eveneens zelfstandig aansprakelijk voor de naleving van de beginselen met betrekking tot de verwerking van persoonsgegevens die zijn opgenomen in de AVG.
De afspraken die De Psychologengroep hierover met de verwerker maakt worden schriftelijk vastgelegd, of in een andere, gelijkwaardige vorm.

3. Doel werkwijze

Het voldoen aan wetgeving door het op een juiste manier omgaan met persoonsgegevens en het verplicht melden van datalekken aan de AP.

4. Verantwoordelijken

- Directie	- maakt afweging of er sprake is van een datalek en of deze gemeld moet worden bij de AP. (is eindverantwoordelijke). Draagt zorg dat datalekken gemeld worden aan AP
- Medewerkers	- melden van datalek aan directie
- Functionaris Gegevensbescherming	- beheren en monitoren van gemelde registraties

5. Proces

Processtap	Verantw.	Verwijzing naar document/richtlijn	Prestatie indicator
1. Afspraken met een Verwerker a. De Psychologengroep heeft vastgelegd wie de specifieke verwerkers zijn van persoonsgegevens. b. De Psychologengroep zorgt ervoor dat de verwerkers maatregelen treffen die nodig zijn, zodat we daarmee aan de meldplicht voor datalekken voldoen. De Psychologengroep maakt afspraken met de verwerker over de volgende zaken en legt deze vast in contracten (of in een addendum): • De verwerker is verplicht De Psychologengroep te informeren over alle relevante incidenten. • De Psychologengroep hoort per incident alle relevante informatie te ontvangen van de verwerker. • Hoe informeert de verwerker De Psychologengroep over de incidenten? • Wanneer precies behoort de verwerker De Psychologengroep te informeren over de incidenten? - De verwerker is verplicht om De Psychologengroep onmiddellijk op de hoogte te houden van eventuele nieuwe ontwikkelingen rond het incident en van de maatregelen die de verwerker treft om aan zijn kant de gevolgen van het incident te beperken en herhaling te voorkomen. - De verwerker moet kunnen aantonen/vaststellen dat De Psychologengroep daadwerkelijk op de hoogte wordt gesteld van alle relevante incidenten, en dat de verstrekte informatie klopt.	Functionaris Gegevensbescherming	Verwerkingenregister Guidelines on Personal data breach notification under Regulation 2016/679	

5.1 Intern melden van een datalek

Processtap	Verantw.	Verwijzing naar document/richtlijn	Prestatie indicator
2. Melden datalek intern • Zodra binnen of door De Psychologengroep een datalek wordt geconstateerd, wordt deze onmiddellijk gemeld aan een de directie. (Indien melding wordt gedaan over poststukken/brieven die op straat gevonden worden, zal al het mogelijke worden gedaan om de post z.s.m. naar kantoor te krijgen) • Het datalek wordt onmiddellijk besproken met de directie. • I.v.m. het beheren en monitoren van de melding, wordt alle informatie (t.a.v. de melding t/m de afhandeling) gelijktijdig toegedaan aan de Functionaris Gegevensbescherming.	Medewerker Directie Directie	Formulier melding datalek (intern)	Dezelfde dag Dezelfde dag Binnen 24 uur Binnen 24 uur
3. Verwerking gegevens datalek • De gegevens m.b.t het datalek worden verzameld en geregistreerd en dienen als input voor verbeteracties en • worden gecommuniceerd aan betrokkenen (in-/extern).	Functionaris Gegevensbescher ming		Binnen 48 uur

5.2 Extern melden van een datalek aan de Autoriteit Persoonsgegevens (AP)

Processtap	Verantw.	Verwijzing naar document/richtlijn	Prestatie indicator
4. **Nagegaan wordt welke specifieke datalekken moeten worden gemeld** Om vast te stellen of een specifiek datalek moeten worden gemeld aan de AP, worden de guidelines gevolgd.	Functionaris Gegevensbescherming i.s.m. Directie	Guide Lines on Personal data breach notification under Regulation 2016/679	Binnen 48 uur
5. **Hoe moet een datalek worden gemeld?** • Het datalek moet worden gemeld aan de AP via een speciaal meldingsformulier van de AP. • De AP stuurt een ontvangstbevestiging na de melding. Bij die meldingen die aanleiding geven tot nadere actie door de AP, zal de AP contact met De Psychologengroep opnemen om de herkomst van de melding te verifiëren.	Directie/Functionaris Gegevensbescherming	Meldingsformulier AP	
6. **Wanneer moet een datalek worden gemeld aan de AP?** Het datalek moet onmiddellijk gemeld worden aan de AP. • **Uiterlijk op de tweede werkdag na de ontdekking van het incident moet de melding worden gedaan**, tenzij op dat moment inmiddels uit onderzoek is gebleken dat het incident niet onder de meldplicht valt. Evt. kan de melding naderhand nog worden aangevuld of ingetrokken. • In de melding aan de AP moet aangeven worden of het datalek al aan de betrokkenen is gemeld en, zo niet, wanneer dat wordt gedaan. • De termijn die we in de melding aan de AP aangeven, moeten we nakomen. Mocht deze termijn bij nader inzien niet haalbaar blijken te zijn, dan moeten we dit aan de AP laten weten d.m.v. een aanpassing van de melding.	Functionaris Gegevensbescherming	AVG: artikel 33	Onverwijld, (uiterlijk op 2e werkdag na incident)

7. **Hoe moet een datalek worden gemeld aan betrokkene(n)?** In de kennisgeving aan de betrokkene moet het volgende worden vermeld: • de aard van de inbreuk • de instanties waar de betrokkene meer informatie over de inbreuk kan krijgen • de maatregelen die we de betrokkene aanbevelen om te nemen, om de negatieve gevolgen van de inbreuk te beperken	Functionaris Gegevensbescherming	AVG: artikel 33, lid 3	
Processtap	Verantw.	Verwijzing naar document/richtlijn	Prestatie indicator
8. **Wanneer moet een datalek worden gemeld aan betrokkene(n)?** Het datalek moet onmiddellijk worden gemeld aan de betrokkene. • In de melding aan de AP moeten aangeven worden of het datalek al aan de betrokkenen is gemeld en, zo niet, wanneer dat wordt gedaan. • De termijn die we in de melding aan de AP aangeven, moeten we nakomen. Mocht deze termijn bij nader inzien niet haalbaar blijken te zijn, dan moeten we dit aan de AP laten weten d.m.v. een aanpassing van de melding.	Functionaris Gegevensbescherming	AVG: artikel 34	Onverwijld / na overleg
9. **Welke gegevens moeten worden vastgelegd over een datalek?** • De Psychologengroep houdt een overzicht bij van alle datalekken die onder de meldplicht vallen. • Per datalek staan in het overzicht in ieder geval de feiten en gegevens omtrent de aard van de inbreuk. • Als het datalek is gemeld aan de betrokkene, dan wordt ook de tekst van de kennisgeving aan de betrokkene in het overzicht opgenomen. (Het is mogelijk dat een vervolgprocedure na een datalek juridische maatregelen kan omvatten (civiel- of strafrechtelijk), en dat we bewijsmateriaal moeten verzamelen, bewaren en presenteren overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd).	Functionaris Gegevensbescherming	'Overzicht datalekken De Psychologengroep' AVG: artikel 33	Bewaartermijn: Minimaal 1 jaar

Processtap	Verantw.	Verwijzing naar document/richtlijn	Prestatie indicator
10. Wat doet de AP met onze melding? Na het melden van een datalek ontvangt De Psychologengroep een ontvangstbevestiging. • Als de melding de AP aanleiding geeft tot nadere actie, dan zal de AP daarover contact met u opnemen. In eerste instantie zal het daarbij gaan om verificatie dat de gedane melding daadwerkelijk van u afkomstig is, en om eventuele inhoudelijke vragen over de melding. • De AP houdt een register bij van de ontvangen datalekmeldingen. Dit register is niet openbaar. • De AP houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens. • De AP kan samenwerkingsafspraken maken met andere toezichthouders. Deze afspraken worden vastgelegd in een samenwerkingsprotocol, dat wordt gepubliceerd in de Staatscourant. • In het kader van deze afspraken kan de AP ook informatie uit ontvangen datalekmeldingen doorgeven aan deze toezichthouders. • Overtreding van de meldplicht datalekken kan worden bestraft met het opleggen van een bestuurlijke boete.	Autoriteit Persoons-gegevens		

5.3 Extern melden van een datalek aan de verzekering

Processtap	Verantw.	Verwijzing naar document/richtlijn	Prestatie indicator
11. Een datalek zal, in geval van mogelijke schadeclaims, gemeld moeten worden aan de verzekering.	Directie		Onverwijld

5.4 Interne communicatie m.b.t. datalekken en beveiligingsincidenten

Processtap	Verantw.	Verwijzing naar document/richtlijn	Prestatie indicator
12. Communicatie binnen De Psychologengroep Het geconstateerde datalek en benodigde acties worden binnen De Psychologengroep gecommuniceerd met: • De betrokken hulpverleners	Directie		Onverwijld