Actieschema: "Wat te doen bij datalekken?"

	Een datalek wil zeggen dat er vanuit of binnen de praktijk persoonsgegevens van patiënten (data) op 'straat' zijn gekomen, door onbevoegden zijn ingezien of verloren gegaan. Hiervoor zijn 3 onderstaande actiepunten voor de praktijk van toepassing.		
1	**Is er daadwerkelijk sprake van een datalek?**	Er is sprake van een datalek als door een inbreuk op de beveiliging, vertrouwelijke gegevens verloren kunnen zijn gegaan, of als niet uitgesloten is dat deze door onbevoegden zijn verwerkt, binnen of buiten de beschermde (Intramed) omgeving van de praktijk.	Voorbeelden: UZI pas met pincode kwijt, inbreuk door een hacker, diefstal van dossiers, fout van een medewerker, fout van een andere zorgpartij of gegevensverwerker.
2	**Moet het lek gemeld worden bij de Autoriteit Persoonsgegevens (AP)?**	Wanneer er cliëntgegevens zijn gelekt zijn we verplicht dit binnen 72 uur na bekend worden te melden bij de AP. Bij twijfel melden we ook. (Een melding kan altijd later weer ingetrokken worden, '*beter het zekere voor het onzekere'* en ten onrechte niet melden kan leiden tot hoge boetes.	Een datalek wordt gemeld via het Meldloket Datalekken van de AP: https://datalekken.autoriteit-persoonsgegevens.nl.actionpage?0
3	**Moeten cliënten geïnformeerd worden?**	Als er cliëntgegevens zijn gelekt worden deze ook z.s.m. maar in ieder geval direct na de melding bij punt 2, geïnformeerd zodat ook zij zo nodig maatregelen kunnen nemen om zich te beschermen tegen de gevolgen van de datalek.	We informeren de cliënt (individueel of in combinatie met algemene voorlichting) over de aard van de inbreuk, de instanties waar de betrokkene meer informatie over de inbreuk kan krijgen, en de maatregelen die we de betrokkene aanbevelen om de mogelijk negatieve gevolgen van de inbreuk, zoals het veranderen van gebruikersnamen en wachtwoorden. De aard van de inbreuk wordt in algemene zin beschreven en onze contactgegevens zijn beken bij de cliënt voor communicatie over het datalek.
4	**Moeten actiepunten geregistreerd worden?**	Wanneer er sprake is van een mogelijk datalek dan wordt deze in een register opgenomen.	Het register is het overzicht van – mogelijke – datalekken en dient ook als uitgangspunt voor verbeteringen in het omgaan met persoonsgegevens.

ALGEMENE VERORDENING GEGEVENSBESCHERMING
Actieschema: "Wat te doen bij datalekken?"
Omgangsnormen informatiebeveiliging

1. Medewerkers mogen niet zelf eigen software downloaden en installeren op bedrijfsapparatuur
Medewerkers en onderaannemers mogen niet op eigen houtje software installeren op voor de praktijk gebruikte hardware. Dit zorgt voor kwetsbaarheden in de databeveiliging. Voor apparaten die toegang hebben tot persoonsgegevens is het niet toegestaan.

2. Bij afgeschreven hardware worden alle persoonsgegevens vernietigd.
Alle persoonsgegevens worden minimaal onleesbaar gemaakt. Data worden overschreven. (Bestanden verwijderen is onvoldoende!) De gegevensdragers worden overschreven, geformatteerd of onbruikbaar gemaakt. Ook mobiele telefoons, scanners en printers worden hierin meegenomen

3. Persoonsgegevens worden verzonden via een beveiligde omgeving.
De praktijk gebruikt Siilo, Zorgmail en Zorgdomein voor het uitwisselen van persoonsgegevens. Wanneer er onverhoopt gebruik van gemaakt van mail door derden dan wordt ook hier middels de bovenstaande mogelijkheden inhoudelijk op gereageerd en zo nodig bijgestuurd.
Daar komt nog bij dat het onwenselijk is dat er bestanden met persoonsgegevens rondzweven in mailboxen, omdat deze data volledig van de radar zijn. Daardoor is deze niet in beeld bij een 'recht om vergeten te worden'-verzoek van een klant of bij een potentieel datalek.

4. De praktijk gebruikt een online omgeving, gefaciliteerd door Intramed.
De praktijk gebruikt geen andere online omgevingen zoals bijv. Google of Microsoft. De door Intramed gefaciliteerde omgeving voldoet aan de door de wetgeving gestelde voorwaarden. Met Intramed is een verwerkingsovereenkomst gesloten zoals voorgesteld in de nieuwe wetgeving.

5. Online webformulieren zijn beveiligd met een gratis SSL- encriptie
De praktijk maakt gebruik van digitaal verkrijgbare aanmeldingsformulieren. Deze hebben een SSL-encryptie en zijn dus niet voor onbevoegden beschikbaar.

6. De praktijk zorgt voor dagelijkse back-ups van gegevens.
De praktijk maakt gebruik van de Online omgeving van Intramed. Hiermee wordt dagelijks voorzien in de back-up van de cliëntgegevens.

7. De praktijk heeft een privacyverklaring opgesteld.
Deze is vermeld op de website. Voor aanmelding worden cliënten hiervan in kennis gesteld alsmede op het aanmeldingsformulier.

8. Gasten, cliënten hebben nog geen toegang tot ons draadloze netwerk.
Ons wifi netwerk is nog niet geschikt voor vertrouwd gebruik door gasten en cliënten van de praktijk.

9. De praktijk werkt met een checklist gegevensbescherming
Deze dient voor de reguliere werkbespreking om de gegevensbescherming adequaat en actueel te houden bij alle – nieuwe – betrokkenen.