Inleiding
Sinds 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing.
Voor Second Opinion Centrum Nederland / PsyM gaat dit reglement over de cliënten/patiënten. In dit privacyreglement wordt aandacht besteed aan de rechten van de cliënt/patiënt. Second Opinion Centrum Nederland / PsyM geeft aan hoe er met persoonsgegevens omgegaan wordt. In hoofdstuk 1 van het kwaliteitshandboek (blz. 6) is het vastgestelde AVG Second Opinion Centrum Nederland / PsyM opgenomen.
Het medisch beroepsgeheim, gedragscode en de formulieren “opvragen van medisch informatie” en “Toestemmingsformulier MDO-overleg” maken ook onderdeel uit van het Privacyreglement.
Dit document geeft u een getrouw beeld van het Privacyreglement zoals dat erbij Second Opinion Centrum Nederland / PsyM uitziet.

Second Opinion Centrum Nederland / PsyM dient over een verwerkingsregister te beschikken als een of meer van de volgende situaties op u van toepassing zijn.

1. Verwerkingsregister verstrekken
De verwerking van persoonsgegevens is niet incidenteel. SocNed verwerkt in de praktijk gegevens met betrekking tot medewerkers, cliënten en patiënten.
Deze gegevens kunnen een hoog risicogehalte inhouden voor de rechten en vrijheden van de personen van wie wij de persoonsgegevens verwerken.
In de publicatie Position paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR leggen de Europese privacy toezichthouders uit hoe zij aankijken tegen de wettelijke uitzonderingen op de verplichting om een verwerkingsregister op te stellen.

2. Informatieverplichtingen
Onder de AVG gelden er nieuwe informatieverplichtingen en nieuwe regels over het werken met toestemming van de patiënt. Second Opinion Centrum Nederland/ PsyM zal over het algemeen ook verplicht zijn om een register van verwerkingsactiviteiten bij te houden, een data protection impact assessment (DPIA) uit te voeren en een functionaris voor de gegevensbescherming (FG) te hebben.

3. Bestaande regels blijven gelden
De bestaande regels over privacy worden door de AVG bevestigd en op onderdelen versterkt. De volgende wetten blijven voor Second Opinion Centrum Nederland/ PsyM gelden:

Wet op de geneeskundige behandelingsovereenkomst (WGBO);
- Wet kwaliteit, klachten en geschillen zorg (Wkkgz)
- Wet op de beroepen in de individuele gezondheidszorg (Wet BIG)
- Zorgverzekeringswet (Zvw)
- Wet marktordening gezondheidszorg (Wmg)
- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
- De AVG-regels gaan ook naast de huidige regels voor het medisch beroepsgeheim bestaan.

4. Maatregelen voor beveiliging
Second Opinion Centrum Nederland/ PsyM dient persoonsgegevens volgens de Algemene verordening gegevensbescherming (AVG) te beveiligen. Dit, om op deze wijze datalekken te voorkomen.

Second Opinion Centrum Nederland/ PsyM heeft hiervoor passende technische en organisatorische maatregelen genomen:
- Om persoonsgegevens te beveiligen maakt Second Opinion Centrum Nederland/ PsyM gebruik van een beveiligde server en software (Medicore en NEDAP). Wekelijks wordt een back-up gemaakt van alle persoonsgegevens
- Alleen bevoegde medewerkers hebben toegang tot de gegevens van cliënten/patiënten.

- Second Opinion Centrum Nederland/ PsyM blijft voortdurend nadenken over een optimale beveiliging en dit is binnen de organisatie een blijvend punt van aandacht.

5. AVG-regels binnen SocNed Holding:

1. Wat zijn persoonsgegevens?
Dit zijn die gegevens die informatie bevatten over een identificeerbaar natuurlijk persoon. Bijvoorbeeld naam, geboortedatum en/of geslacht.

2. Voor wie van toepassing?
Het privacyreglement geldt voor iedere cliënt/patiënt van SocNed Holding.

3. Doel van dit reglement?
Het geeft duidelijkheid over de wijze waarop Second Opinion Centrum Nederland / PsyM met persoonlijke gegevens van cliënten omgaat.

4. Hoe wordt informatie verkregen?
Informatie over de cliënt/patiënt wordt direct verkregen bij aanmelding van de cliënt/ bij SocNed Holding. Tijdens het behandelingstraject kunnen zich mutaties voordoen. Bijvoorbeeld wijzigingen in de levenssfeer, te denken aan geboorte, overlijden etc. Deze mutaties worden in samenspraak met de cliënt/patiënt verwerkt. Hiervoor is ‘het Toestemmingsformulier’ ontwikkeld met informatie over:

1. Opvragen medisch informatie
2. MDO-richtlijnen
3. Toestemmingsverklaring omtrent inzage dossier

5. Second Opinion Centrum Nederland / PsyM verwerkt ook bijzondere gegevens
Bijzondere gegevens worden geregistreerd of verwerkt, zoals over:

- Godsdienst
- Ras
- Politieke gezindheid
- Gezondheid
- Seksuele leven
- Lidmaatschap van een vakvereniging
- Strafrechtelijke gegevens (indien van toepassing bij aanmelding)
- Persoonsgegevens over onrechtmatig of hinderlijk handelen waarvoor een verbod is opgelegd
- Allemaal met het doel om zorgverlening op maat te kunnen leveren aan de cliënt/patiënt.

6. Waarom wordt de informatie gevraagd?
Persoonsgegevens worden om verschillende redenen gevraagd. Allereerst om ervoor te zorgen dat de cliënt/patiënt goede passende zorg ontvangt. Vervolgens om ook te kunnen voldoen aan wettelijke verplichtingen. Tot slot om een goede interne bedrijfsvoering en een goed organisatie- en zorgbeleid te kunnen voeren.

7. Wie heeft toegang tot de gegevens?
De cliënten/patiëntendossiers worden door de behandelaren/zorgverleners beheerd. Alleen bevoegde personen bij Second Opinion Centrum Nederland / PsyM hebben toegang tot het dossier van een cliënt/patiënt.
Alle behandelaars en zorgverleners hebben in principe toegang tot het digitale patiëntendossier. Elke behandelaar/zorgverlener heeft een eigen inlognaam en wachtwoord waarmee hij of zij via NEDAP en Medicore kan inloggen. Alle dossiers zijn opgeslagen op een beveiligde server van SocNed Holding.

8. Welke rechten heeft de cliënt/patiënt?

- Het recht om te weten dat gegevens worden geregistreerd
- Het recht om kennis te nemen van datgene wat geregistreerd is

- Het recht om te verzoeken gegevens te doen corrigeren, aan te vullen of te verwijderen
- Het recht te weten of en welke gegevens aan derden zijn doorgegeven.

De rechten van patiënten met betrekking tot hun medisch dossier staan deels in de WGBO, deels in de AVG beschreven. Ook in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg zijn bepalingen opgenomen over de rechten van patiënten.
Patiënten hebben het recht hun medisch dossier in te zien en om correctie, aanvulling, of vernietiging van hun dossier te vragen. Ook kunnen zij vragen hun gegevens over te dragen (recht op dataportabiliteit). De gegevens in het dossier, behoren bekend te zijn bij de cliënt/patiënt. De gegevens worden door de cliënt of door een vertrouwd persoon aangeleverd. Daarom wordt ervan uitgegaan dat hij/zij op de hoogte is van de inhoud en dat deze gegevens worden verwerkt.

9. Verstrekken van gegevens aan derden en bewaartermijn
Persoonlijke gegevens mogen niet zomaar aan derden worden verstrekt. De hoofdregel is dat er gegevens mogen worden verstrekt indien dit:

- Voortvloeit uit het doel van de registratie
- Wordt vereist ingevolge van een wettelijk voorschrift
- Geschiedt met toestemming van de cliënt.

De hoofdregel voor het bewaren van medische dossiers staat in de WGBO. In die wet is bepaald dat de zorgverlener het medisch dossier in principe 15 jaar moet bewaren.

10. Waar moet een hulpverlener rekening mee houden?
De gegevens dienen zo te zijn opgeslagen en verwerkt dat ze beveiligd zijn tegen verlies, aantasting, onbevoegde kennisneming, wijziging of verstrekking. Alle dossiers zijn gedigitaliseerd. Als persoonlijke informatie over cliënten ergens mee naartoe wordt genomen dan wordt deze meegedragen in een afgesloten tas of koffer.
Privacygevoelige gegevens over cliënten dienen uitsluitend per fax of via de ZorgMail te worden verstuurd als de ontvanger aanwezig is.

6. Omgaan met het medisch beroepsgeheim
Second Opinion Centrum Nederland / PsyM heeft in alle contracten van haar medewerkers het volgende beroepsgeheim op laten nemen:
Geheimhoudingsverklaring
De werknemer erkent dat hem strikte geheimhouding is opgelegd, zowel tijdens als na beëindiging van de onderhavige arbeidsovereenkomst, ter zake van alle gegevens respectievelijk bijzonderheden m.b.t. de onderneming c.q. instelling van werkgever - of een met haar gelieerde onderneming c.q. instelling - betreffende, waarvan werknemer het vertrouwelijke karakter kent of behoort te kennen. Deze plicht tot geheimhouding geldt tevens ten aanzien van de gegevens respectievelijk bijzonderheden van de relaties, opdrachtgevers en/of cliënten van werkgever en/of de met haar gelieerde ondernemingen c.q. instellingen betreffende.

7. Datalek
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. Onder een ‘datalek’ valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens.

7.1 Definities [1]

Autoriteit Persoonsgegevens (AP): de toezichthoudende autoriteit, de onafhankelijke instantie die erover waakt dat persoonsgegevens zorgvuldig en veilig worden verwerkt en zo nodig sancties kan opleggen als dat niet gebeurt.

[1] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

Bestand: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn.

Betrokkene: degene op wie een persoonsgegeven betrekking heeft, meestal de cliënt, of zijn (wettelijk) vertegenwoordiger.

Bijzondere categorieën persoonsgegevens: persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Derde: elke persoon of instantie die geen betrokkene, verwerkingsverantwoordelijke, verwerker, of een persoon is die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd is persoonsgegevens te verwerken.

Functionaris voor gegevensbescherming (FG): functionaris die door de zorgaanbieder moet of kan worden aangesteld voor het informeren en adviseren over en het toezicht houden op de toepassing en naleving van de AVG en andere gegevensbeschermingsbepalingen. PsyM heeft de contactgegevens van de functionaris voor gegevensbescherming bekend gemaakt bij de Autoriteit Persoonsgegevens. Binnen PsyM is Seyyit Karasoylu (alg. directeur) als functionaris voor gegevensbescherming werkzaam.

Gezondheidsgegevens: gegevens over de lichamelijke of geestelijke gezondheid van een persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven;

Inbreuk in verband met persoonsgegevens: 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. Onder een ‘datalek’ valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens.

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Pseudonimisering: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkenen kunnen worden gekoppeld zonder dat aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

Toestemming van de betrokkene: door betrokkene, op goede informatie berustende, specifieke, in vrijheid en ondubbelzinnig gegeven toestemming waarbij betrokkene hem betreffende verwerking van persoonsgegevens aanvaardt. Dat kan door middel van een schriftelijke of mondelinge verklaring of een ondubbelzinnige actieve handeling (zoals het elektronisch aanvinken van een hokje).

Verwerker: degene die in opdracht van en voor de verwerkingsverantwoordelijke persoonsgegevens verwerkt (bijvoorbeeld een externe hostingsfirma, saas-leverancier, kwaliteitsauditor of een extern salarisadministratiekantoor).

Verwerking van persoonsgegevens: alle handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of in een andere vorm beschikbaar stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Verwerkingsverantwoordelijke: degene die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; meestal de bestuurder van de zorgaanbieder.

7.2 Vertegenwoordiging

1. Is de betrokkene ouder dan achttien jaar en wilsonbekwaam ter zake, dan treedt als vertegenwoordiger voor hem op:
    a) een (toegewezen) curator of mentor;
    b) indien er geen curator of mentor is, de persoon die de cliënt schriftelijk heeft gemachtigd;
    c) indien de persoonlijk gemachtigde ontbreekt of niet optreedt; de echtgenoot of levensgezel van de betrokkene;
    d) indien de echtgenoot of levensgezel ontbreekt of niet optreedt: een kind, broer of zus van de betrokkene.
2. Indien nodig zoekt PsyM samen met de desbetreffende Gemeente waar client woont en kijkt in haar netwerk dat er zo snel mogelijk een wettelijk vertegenwoordiger voor betrokkene optreedt. Zo nodig, als familie of naaste dat niet kan of wil, verzoekt hij de rechter om een vertegenwoordiger te benoemen.

7.3 Verantwoordelijkheid van de verwerkingsverantwoordelijke

1. Gelet op de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft PsyM passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.

2. PsyM hanteert gedragscodes en goedgekeurde ISO-certificering als element om aan te tonen dat we de verplichtingen zijn nagekomen.

7.4 Gegevensbescherming door ontwerp en standaardinstellingen

1. Rekening houdend met de stand van de methode, de uitvoeringskosten, en de aard, de bereik, de context en het doel van de verwerking alsook met de qua bedoening en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden, treft PsyM, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, zoals pseudonimisering, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals allerminste gegevensverwerking, op een effectieve manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen.

2. PsyM treft passende bedrevene en constructieve maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan. Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.

   Bovenstaande houdt in dat:

   a) PsyM streeft ernaar te werken volgens de voor de veilige verwerking van zorggegevens de normen van de NEN-EN-ISO 9001.

   b) Voor de verstrekking van gegevens via e-mail wordt gebruik gemaakt van de beveiligde e-mailverbinding (zorgmail).

   c) De identificerende gegevens zijn zoveel als mogelijk gescheiden opgeslagen van de inhoudelijke gegevens, gepseudonimiseerd of versleuteld.

   d) De standaardinstellingen zijn nee, tenzij (opt-in) in plaats van ja, mits (opt-out), tenzij de wetgeving opt-out toelaatbaar stelt.

   e) PsyM hanteert per verwerking een autorisatieprotocol. Daarin staat welke gegevens door wie/welke (groepen) medewerkers verwerkt kunnen worden en waarom en welke bevoegdheden zij hebben ten aanzien van welke gegevens (inzage, toevoegen, wijzigen, verwijderen).

7.5 Gezamenlijke verwerkingsverantwoordelijken

1. Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken. Zij stellen op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van deze AVG vast, ten aanzien van de uitoefening van de rechten van de betrokkene en hun respectieve verplichtingen om de verplichte informatie te verstrekken, door middel van een onderlinge regeling. In de regeling kan een contactpunt voor betrokkenen worden aangewezen. [2]

2. Uit de bedoelde regeling blijkt duidelijk welke rol de gezamenlijke verwerkingsverantwoordelijken respectievelijk vervullen, en wat hun respectieve verhouding met de betrokkenen is. De wezenlijke inhoud van de regeling wordt aan de betrokkene beschikbaar gesteld.

3. Ongeacht een dergelijke regeling kan een betrokkene zijn rechten uit de AVG met betrekking tot en jegens iedere verwerkingsverantwoordelijke uitoefenen.

7.6 Register van verwerkingen

[2] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verwerkers

1. PsyM houdt een register bij van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden. Dat register bevat in ieder geval de volgende gegevens:

   a) de naam en de contactgegevens van PsyM en eventuele gezamenlijke verwerkingsverantwoordelijken, en van de functionaris voor gegevensbescherming;
   b) de verwerkingsdoeleinden;

   c) een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;

   d) de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;
   e) indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, van de AVG bedoelde doorgiften, de documenten inzake de passende waarborgen;

   f) indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;

   g) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

2. De verwerker en, in voorkomend geval, de vertegenwoordiger van de verwerker houdt een register van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van een verwerkingsverantwoordelijke hebben verricht. Dit register bevat de volgende gegevens:

   a) de naam en de contactgegevens van de verwerkers en van iedere verwerkingsverantwoordelijke voor rekening waarvan de verwerker handelt en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke of de verwerker en van de functionaris voor gegevensbescherming;
   b) de categorieën van verwerkingen die voor rekening van iedere verwerkingsverantwoordelijke zijn uitgevoerd;

   c) indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, onder vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, eerste lid, tweede alinea, van de AVG bedoelde doorgiften, de documenten inzake de passende waarborgen;

   d) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.
3. Het register is in schriftelijke vorm, waaronder in elektronische vorm, opgesteld.

4. Desgevraagd stellen de verwerkingsverantwoordelijke of de verwerker het register ter beschikking van de Autoriteit Persoonsgegevens.

7.6 Medewerking verlenen aan/samenwerken met de Autoriteit persoonsgegevens

PsyM en de verwerker en, in voorkomend geval, hun vertegenwoordigers, werken desgevraagd samen met de Autoriteit Persoonsgegevens bij het vervullen van haar taken.

7.7 Verwerker

1. AVG-eisen verwerkingsverantwoordelijken en verwerkers. Als verwerkingsverantwoordelijke blijft PsyM altijd verantwoordelijk voor de persoonsgegevens die verwerkt. Ook wanneer PsyM die verwerking uitbesteedt aan verwerkers. Onze cliënten/patiënten/gemeentes etc. hebben hun persoonsgegevens immers met ons gedeeld. En niet met onze verwerkers. Maar dat betekent niet dat wij als verwerker geen verantwoordelijkheden heeft. Ook PsyM moet aan bepaalde AVG-regels voldoen. Opdrachtgevers kunnen dat ook van ons verwachten. PsyM onderscheidt zich bovendien positief wanneer wij laat zien dat wij de AVG-regels kent en daaraan voldoet.

2. Is PsyM verwerkingsverantwoordelijke of verwerker?
   In de praktijk kan het soms lastig zijn om te bepalen of PsyM verwerker of verwerkingsverantwoordelijke is. Op de website van de AP is een voorbeeld lijst: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/voorbeeldlijst_verwerkers_def.pdf

1. Verwerkersovereenkomst
   Verwerkingsverantwoordelijken en verwerkers moeten samen een verwerkersovereenkomst afsluiten. Doen zij dat niet? Dan zijn beide partijen in overtreding.

7.7 Beveiliging van de verwerking

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen PsyM en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:
   a) de pseudonimisering en versleuteling van persoonsgegevens;

   b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;

   c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;

   d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

2. Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, met name als gevolg van

   1. Vernietiging, verlies, wijziging of ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

2. Het aansluiten bij een goedgekeurde gedragscode of een goedgekeurd certificeringsmechanisme kan worden gebruikt als element om aan te tonen dat de in lid 1 van dit artikel bedoelde vereisten worden nageleefd.

3. PsyM en de verwerker treffen maatregelen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van PsyM of van de verwerker en toegang heeft tot persoonsgegevens, deze slechts in opdracht van de zorgaanbieder verwerkt, tenzij hij daartoe volgens wet- en regelgeving is gehouden.

7.8 Datalek melden

Second Opinion Centrum Nederland/ PsyM dient de datelek te melden. De meldplicht datalekken houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) zodra zij een ernstig datalek hebben. En soms moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). [3]

Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Of zonder dat dit wettelijk is toegestaan.

Datalek melden

Indien een medewerker van PsyM die een datalek willen melden bij de AP, kunnen dat doen via het meldloket datalekken. In de privacyverklaring datalek melden staat hoe de AP omgaat met de persoonsgegevens van degene die een datalek meldt.

7.9 Stappenplan Datalek

Stappenplan: kom in actie bij een datalek [4]
Zie volgende pagina.

[3] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

[4] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stappenplan_kom_in_actie_bij_een_datalek.pdf

Stap 1: zorg voor overzicht

Analyseer onmiddellijk de situatie. Zorg dat u weet wat er is gebeurd en wat de omvang van het lek is. Gaat het om een inbreuk door gelekte, vernietigde of gewijzigde gegevens? Indien gegevens zijn gelekt, onderzoek dan wie er (mogelijk) toegang hebben (gehad) tot welke persoonsgegevens. Deze informatie heeft u nodig voor de vervolgstappen.

Stap 2: Beperk de schade!

Bepaal op basis van stap 1 of er maatregelen zijn die u meteen kunt nemen om het datalek te beëindigen en de schade te beperken. En zo ja, neem deze maatregelen onmiddellijk. Bijvoorbeeld door een gestolen laptop op afstand te wissen. Maak tegelijkertijd een inschatting van het (mogelijke) risico dat het datalek oplevert (stap 3).

Stap 3: Wel/niet melden bij de AP

Bepaal of u het datalek verplicht moet melden bij de Autoriteit Persoonsgegevens (AP). Zo ja, zorg dat u dit ***binnen 72 uur*** nadat u het lek heeft ontdekt doet. U moet een datalek melden bij de AP tenzij het niet waarschijnlijk is dat het datalek een risico oplevert voor de rechten en vrijheden van de betrokken personen.

Heeft u bij de eerste melding nog niet alle informatie over het datalek?
Doe dan een eerste melding binnen 72 uur en doe later een vervolgmelding.

Naar het meldloket datalekken
Zie ook: voorbeeldlijst 'datalek wel/niet melden bij AP en betrokkenen'

Stap 4: Wel/niet melden aan de betrokken personen

Bepaal of u het datalek verplicht moet melden aan de betrokken personen. Zo ja, zorg dat u dit zo snel mogelijk doet. U moet een datalek melden aan de betrokken personen wanneer er sprake is van een *hoog* risico voor de rechten en vrijheden van de betrokken personen.

Stap 5: Registreer het datalek

Registreer het datalek in uw verplichte datalekregister. Ook wanneer u het datalek niet meldt aan de AP.

Zie ook: 10 praktische tips voor betere datalekregistratie