



Privacyverklaring persoonsgegevens

Januari 2020

Privacyverklaring IJsselgroep

Artikel 1: Begrippen

- A. AVG: de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 (Algemene Verordening Gegevensbescherming).
- B. Bestand: elk gestructureerd geheel van Persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.
- C. Betrokkene: de persoon op wie een Persoonsgegeven betrekking heeft, zoals het kind, wettelijk vertegenwoordigers, leraren, directeuren en/of bestuurders van scholen.
- D. Bijlage: de bijlage bij deze Verklaring.
- E. Datalek: elke inbreuk op de beveiliging, zoals bedoeld in artikel 32 AVG, die waarschijnlijk nadelige gevolgen heeft voor de rechten en vrijheden van natuurlijke personen dan wel nadelige gevolgen heeft voor de bescherming van Persoonsgegevens die door Verwerker worden verwerkt, zoals bedoeld in artikel 33 AVG.
- F. Derde: ieder, niet zijnde de betrokkene, de Verwerkingsverantwoordelijke, de Verwerker, of enig persoon die onder rechtstreeks gezag van de Verwerkingsverantwoordelijke of de Verwerker gemachtigd is om Persoonsgegevens te verwerken.
- G. OAB: het Onderwijsadviesbureau, genaamd IJsselgroep, gevestigd te 2^e Wormenseweg 80 te Apeldoorn.
- H. Ontvanger: degene aan wie de Persoonsgegevens worden verstrekt.
- I. Persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.
- J. Toestemming van de betrokkene: elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende Persoonsgegevens worden verwerkt.
- K. Verklaring: deze privacyverklaring.
- L. Verwerker: degene die ten behoeve van de Verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.
- M. Verwerking van Persoonsgegevens: een bewerking of een 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 Persoonsgegevens.
- N. Verwerkingsverantwoordelijke: degene die het doel van en de middelen voor de Verwerking van Persoonsgegevens vaststelt.
- O. Verstrekken van persoonsgegevens: het bekend maken of ter beschikking stellen van Persoonsgegevens.
- P. Verzamelen van persoonsgegevens: het verkrijgen van Persoonsgegevens.

Artikel 2: Toepasselijkheid verklaring, rechtsverhouding

1. Deze Verklaring is bedoeld voor de ouder/voogd/leerling die het OAB een opdracht¹ of behandelovereenkomst verstrekt voor screening, diagnostiek en/of behandeling van een leerling m.b.t. dyslexie-problematiek en behandeling van/begeleiding bij lichte gedragsproblematiek.
2. De Verklaring is voorts te raadplegen op <https://www.ijsselgroep-ed.nl/privacyverklaring>

Artikel 3: Categorieën van Betrokkenen wiens gegevens kunnen worden verwerkt.

1. De verwerking van Persoonsgegevens bevat gegevens over de volgende categorieën van Betrokkenen:
 - a. kinderen²;
 - b. ouders, verzorgers en/of voogden of wettelijk vertegenwoordigers van kinderen;
 - c. leraren, directeuren, bestuursleden en/of andere werknemers van scholen;
 - d. onderwijsprofessionals (al dan niet extern ingeschakeld).
2. Gegevens over de in lid 1 sub b, c en d genoemde personen worden uitsluitend verwerkt indien dat noodzakelijk is voor de oplossing van het probleem van de leerling.

¹ Waar in deze Verklaring opdracht staat kan ook behandelovereenkomst worden gelezen.

² Waar in deze verklaring kind staat kan ook jongeren of leerling worden gelezen

Artikel 4: Soorten van gegevens die kunnen worden verwerkt en de wijze van verkrijging

1. De (Persoons)gegevens die, afhankelijk van het doel van de opdracht, kunnen worden verwerkt, betreffen:
 - a. de gegevens van het kind die op het aanmeldingsformulier staan vermeld;
 - b. gegevens betreffende de aard en de omvang van het probleem waar de betreffende kind mee te maken heeft, zoals:³
 - i. de informatie welke het OAB met toestemming van leerling/ouders/voogd ontvangt van de school, verband houdende met de problematiek van het kind
 - ii. de informatie welke het OAB met toestemming van leerling/ouders/voogd ontvangt van andere partijen zoals logopedie, Bureau Jeugdzorg, GGD/Jeugdarts/GGZ/Medisch specialist of anderszins, verband houdende met de problematiek van het kind
 - iii. verslagen van eventuele eerdere observaties van andere instanties, welke het OAB met toestemming van leerling/ouders/voogd ontvangt
 - iv. de gegevens welke OAB zelf verzamelt gedurende het onderzoek naar de problematiek van het kind en gedurende het aanbieden van de behandeling aan het kind, zoals (gespreks)verslagen, uitkomsten van testen, (onderzoeks)rapportages etc.

Artikel 5: Waarvoor en op welke grond Persoonsgegevens verwerkt worden

1. Het OAB verwerkt persoonsgegevens met de volgende doelen:
 - a. het onderzoeken van de problematiek met als doel te komen tot de juiste diagnose (screening en diagnostiek);
 - b. het aanbieden van de een passende behandeling van de problematiek;
 - c. het aanvragen van een vergoeding bij de gemeente voor het verlenen van de benodigde zorg;
2. De verwerking van persoonsgegevens vindt plaats op basis van minimaal een van de volgende grondslagen:
 - a. Verwerking is noodzakelijk voor de uitvoering van een overeenkomst;
 - b. De betrokkene heeft toestemming gegeven voor de verwerking van de persoonsgegevens voor een specifiek doeleinde;
 - c. Verwerking is noodzakelijk om een wettelijke verplichting na te komen waaraan de Verwerkingsverantwoordelijke onderworpen is
 - d. Verwerking is noodzakelijk ter bescherming van een vitaal belang van de Betrokkene;
 - e. Verwerking is noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de Verwerkingsverantwoordelijke zoals vermeld in artikel 10, tenzij het belang of de fundamentele rechten en vrijheden van de Betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.
3. Het weigeren van het verstrekken van Persoonsgegevens van en door Betrokkenen voor de verwerking van de onder sub 2 a) genoemde gegevens kan gevolgen hebben voor de uitvoering van de dienstverlening. OAB zal opdrachtgever hierover in dat geval informeren.

Artikel 6: Hoe lang Persoonsgegevens verwerkt worden

1. De Persoonsgegevens worden na afronding van de behandeling nog 15 jaar bewaard, zoals is bepaald in de Jeugdwet.

Artikel 7: Verwerking Persoonsgegevens

1. De Persoonsgegevens zullen uitsluitend worden opgeslagen en verwerkt binnen de Europese Economische Ruimte (EER).

Artikel 8: Geheimhouding

1. Het OAB verplicht de personen die in haar dienst zijn, dan wel werkzaamheden voor haar verrichten, tot geheimhouding met betrekking tot al hetgeen waarvan zij met betrekking tot de uitvoering van een opdracht voor een school of wettelijk vertegenwoordiger van een leerling kennis kunnen nemen. Indien dit voor voornoemde personen niet reeds contractueel is vastgelegd, zal het OAB deze personen een geheimhoudingsverplichting opleggen voor de Persoonsgegevens waarvan zij kennis zullen nemen. Deze verplichting zal schriftelijk worden vastgelegd en een kopie daarvan zal op eerste verzoek de wettelijk vertegenwoordiger van en/of een leerling ter inzage worden aangeboden.

³ Hieronder valt tevens ruw onderzoeksmateriaal, zoals met de hand geschreven aantekeningen die worden opgeslagen in een bestand.

2. De Verwerkers welke door het OAB zijn ingeschakeld bieden afdoende garantie met betrekking tot toepassing van passende technische en organisatorische maatregelen, zodat aan de vereisten van de AVG wordt voldaan en de bescherming van de rechten van betrokkenen zijn gewaarborgd. De afspraken hierover met Verwerkers worden telkens vastgelegd in een zogenaamde verwerkersovereenkomst. De uitwisseling van gegevens inzake de Nederlandse Databank Dyslexie (NDD), zoals vermeld in artikel 10, valt hier ook onder (betreft uitwisseling met verwerker Stichting CED-Groep).

Artikel 9: Verstrekking aan derden

1. Het OAB zal onder geen omstandigheden de Persoonsgegevens delen met of verstrekken aan Derden, tenzij het OAB daartoe voorafgaande, uitdrukkelijk schriftelijke toestemming van leerling/ouders/voogd toestemming heeft verkregen. Uitzondering hierop vormen dwingendrechtelijke wettelijke regels welke het OAB verplichten om gegevens aan derden te verstrekken.

Artikel 10: Nederlandse Databank Dyslexie

1. Om het kind de juiste en beste zorg te geven, werkt het OAB mee aan de verbetering van de kwaliteit van die zorg. Het OAB heeft daartoe ook een wettelijke plicht. Hiervoor werkt het OAB in een collectief samen met het Nederlands Kwaliteitsinstituut Dyslexie (hierna: NKD). Samen met het NKD is de Nederlandse Databank Dyslexie (hierna: NDD) ingericht. In deze databank worden gegevens verzameld over o.a. diagnostiek en resultaten van alle behandelingen (naast gegevens over de behandeling betreft dit: cliëntnummer, BRIN-nummer school, groep/leerjaar, geboortedatum, geslacht). Om de privacy van Betrokkenen te waarborgen heeft het OAB (in een collectief) tezamen met NKD een verwerkingsovereenkomst afgesloten met Stichting CED-Groep, welke vergaande beveiligingsmaatregelen heeft getroffen en de gegevens in de databank voor het NKD anonimiseert. De gegevens in het NDD zijn hierdoor door NKD niet te herleiden tot Betrokkenen (en zijn daardoor geen persoonsgegevens meer). Naast kwaliteitsverbetering kunnen de (geanonimiseerde) gegevens gebruikt worden voor voorlichting, wetenschappelijke onderzoek en maatschappelijke verantwoording.
2. De grondslag voor deze gegevensverwerking is het gerechtvaardigd belang van het OAB om op deze wijze invulling te geven aan haar wettelijke plicht om gegevens over kwaliteit van zorg te registreren. Dit naast het belang om de (geanonimiseerde) gegevens te gebruiken voor voorlichting, wetenschappelijk onderzoek en maatschappelijke verantwoording.
3. Betrokkenen hebben ten allen tijde het recht om – vanwege redenen die verband houden met hun specifieke situatie – bij het OAB bezwaar te maken tegen deze gegevensverwerking. In dat geval zullen de gegevens niet in de databank worden opgenomen of uit de databank worden verwijderd. De door het OAB aanleverde gegevens worden door Stichting CED-Groep na 3 jaar verwijderd. De geanonimiseerde gegevens in het NDD worden maximaal 7 jaar bewaard.

Artikel 11: Beveiligingsmaatregelen het beheer van de verwerking van persoonsgegevens

1. Het OAB zal – rekening houdend met de van toepassing zijnde regelgeving op het gebied van bescherming van persoonsgegevens, de stand van de techniek en de kosten van tenuitvoerlegging – technische en organisatorische beveiligingsmaatregelen treffen om te zorgen voor beschikbaarheid, integriteit en vertrouwelijkheid van de Persoonsgegevens en om de Persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige Verwerking. De beveiligingsmaatregelen van het OAB zullen worden beschreven in Bijlage 1 bij deze Verklaring.

Artikel 12: Registerplicht

1. Het OAB houdt als Verwerkingsverantwoordelijke een register bij zoals bedoeld in artikel 30 lid 1 AVG. Tenzij er sprake is van de uitzondering zoals genoemd in artikel 30 lid 5 AVG.
2. Het register bevat alle verwerkingsactiviteiten die onder verantwoordelijkheid van de Verwerkingsverantwoordelijke worden.
3. Dit register bevat naast hetgeen bepaald in lid 2 ten minste de volgende gegevens:
 - a. de naam en contactgegevens van de Verwerkingsverantwoordelijke en Verwerker, diens vertegenwoordigers en indien van toepassing diens functionarissen voor gegevensbescherming;
 - b. de verwerkingsdoeleinden;
 - c. een beschrijving van de categorieën van betrokken Verwerkers en de categorieën van Persoonsgegevens;
 - d. de categorieën van Ontvangers aan wie de Persoonsgegevens zijn of zullen worden verstrekt;
 - e. indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
 - f. een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen die zijn uitgevoerd.

Artikel 13: Vragen, klachten en uitoefening van rechten

1. Betrokkene heeft diverse rechten, zoals in de navolgende artikelen is te lezen. Als Betrokkene deze rechten wil uitoefenen of vragen of klachten hebben op het gebied van privacybescherming, dan kunnen deze gericht worden aan het OAB via: info@ijsselgroep.nl of 088 093 16 16 (Janna de Haan)

Artikel 14: Inzagerecht

2. De Betrokkene heeft het recht om zich tot het OAB te wenden met het verzoek hem mede te delen of hem betreffende Persoonsgegevens worden verwerkt. Het OAB deelt de Betrokkene schriftelijk binnen 4 weken mee:
 - a. of hem betreffende Persoonsgegevens worden verwerkt; en zo ja
 - b. een volledig overzicht daarvan;
 - c. de doeleinden voor Verwerking;
 - d. de categorieën van gegevens waarop de Verwerking betrekking heeft en de ontvangers of categorieën van ontvangers, alsmede de beschikbare informatie over de herkomst van de gegevens.Het OAB kan in geval van een veelomvattend verzoek binnen 4 weken laten weten dat zij meer tijd nodig heeft voor behandeling van het verzoek, met een maximum van 8 extra weken.
3. Voor het OAB de onder lid 1 bedoelde mededeling doet, stelt zij derden die naar verwachting bedenkingen zullen hebben tegen de mededeling in de gelegenheid hun zienswijze naar voren te brengen indien de mededeling gegevens bevat die hem betreffen, tenzij dit onmogelijk blijkt of een onevenredige inspanning kost.
4. Anderen dan Betrokkenen kunnen slechts inzage vragen na overlegging van een schriftelijke voldoende machtiging die door de Betrokkene of diens wettelijk vertegenwoordiger is verstrekt, voorzien van een voldoende onderbouwing van het verzoek.

Artikel 15: Verzoek tot verbetering, aanvulling of verwijdering

1. De Betrokkene kan het OAB verzoeken de hem betreffende Persoonsgegevens te verbeteren, aan te vullen, te verwijderen, of af te schermen, indien deze feitelijk onjuist zijn, voor het doel of de doeleinden van de Verwerking onvolledig of niet ter zake dienen zijn, dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt.
2. Binnen vier weken na ontvangst van het in lid 1 bedoeld verzoek bericht het OAB de verzoeker schriftelijk of dan wel in hoeverre aan het verzoek wordt voldaan. Een weigering om aan het verzoek te voldoen wordt met redenen omkleed.
3. Een eventuele beslissing tot verbetering, aanvulling, verwijdering of afscherming wordt zo spoedig mogelijk uitgevoerd door het OAB.
4. Het OAB stelt Derden aan wie de gegevens daaraan voorafgaand zijn verstrekt, zo spoedig mogelijk in kennis van de verbetering, aanvulling, verwijdering of afscherming van de gegevens, tenzij dit onmogelijk blijkt of een onevenredige inspanning kost.
5. Het OAB laat aan Betrokkene die het verzoek heeft ingediend op zijn verzoek weten aan wie hij de mededeling genoemd in lid 4 heeft gedaan.

Artikel 16: Overige rechten Betrokkene

1. Voor zover de (privacy)belangen van derden zich daar niet tegen verzetten, heeft de Betrokkene het recht het OAB te verzoeken:
 - a. verdere Verwerking van zijn of haar Persoonsgegevens te beperken of te staken;
 - b. tot overdracht van de Persoonsgegevens die het OAB betreffende Betrokkene heeft verwerkt ten behoeve van de uitvoering van de opdracht dan wel met toestemming van Betrokkene. Hieraan kan het OAB voorwaarden stellen.
2. De Betrokkene heeft het recht om eerder gegeven Toestemming voor de Verwerking van Persoonsgegevens in te trekken.
3. De Betrokkene heeft het recht om over de Verwerking van zijn of haar Persoonsgegevens een klacht in te dienen bij de Autoriteit Persoonsgegevens, te bereiken via <https://autoriteitpersoonsgegevens.nl/>.

Artikel 17: Verwijdering van gegevens

1. Persoonsgegevens zullen worden verwijderd door:
 - a. het permanent wissen van de Persoonsgegevens op de gegevensdragers waarop deze zijn vastgelegd;
 - b. vernietiging van eventuele fysieke kopieën van de Persoonsgegevens waarover het OAB beschikt.
2. Tenzij een wettelijke bewaartermijn anders bepaalt, zal het OAB Persoonsgegevens binnen één kalenderjaar verwijderen nadat de opdracht van de leerling aan het OAB is geëindigd, dan wel binnen één kalenderjaar nadat het laatste contact tussen het OAB en de leerling of diens wettelijk vertegenwoordiger heeft plaatsgehad.
3. Op uitdrukkelijk schriftelijk verzoek van de leerling en/of diens wettelijk vertegenwoordiger, kan het OAB de Persoonsgegevens overgedragen aan een andere (hulpverlenings-)instantie.

Artikel 18: Wijzigingen en aanvullingen Verklaring

1. Het OAB heeft het recht om de bepalingen uit de Verklaring te wijzigen. Betrokkenen zullen in dat geval geïnformeerd worden over de aangepaste verklaring.

Artikel 20: Overige

1. Mochten er vragen zijn naar aanleiding van deze Verklaring, dan kan contact opgenomen worden met het OAB via info@ijsselgroep.nl of via 088 093 16 16.

BIJLAGE 1 - BEVEILIGINGSMAATREGELEN

Zoals opgenomen in artikel 10 van de privacyverklaring treft verwerker passende technische en organisatorische maatregelen om de Persoonsgegevens te beschermen tegen verlies, onrechtmatige verwerking of onrechtmatige toegang. Een en ander rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging van deze maatregelen. De maatregelen worden in deze bijlage beschreven.

Algemene informatie over getroffen beveiligingsmaatregelen

IJsselgroep heeft voor het juiste gebruik van (persoons)gegevens beleid geformuleerd, dat actief wordt uitgedragen, en gegevensstromen in kaart gebracht om met maatregelen te zorgen voor:

1. Beschikbaarheid van gegevens op het juiste moment.
2. Integriteit van gegevens: het waarborgen van de correctheid en de volledigheid van informatie en verwerking waardoor informatie met de werkelijkheid in overeenstemming is en niets ten onrechte is achtergehouden of verdwenen.
3. Vertrouwelijkheid van gegevens: het waarborgen dat informatie alleen beschikbaar is voor degenen die hiertoe geautoriseerd zijn.

(Persoons)gegevens worden alleen gedurende de periode van de werkzaamheden, dus tijdelijk, opgeslagen. De mate van specificiteit en persoonsgerichtheid bepaalt de mate van de gegevensbeveiliging. In sommige gevallen wordt gebruik gemaakt van filmbeelden waarbij apart om toestemming voor doeleinden voor verwerking wordt gevraagd. In andere gevallen worden slechts persoonlijke aantekeningen gemaakt of wordt helemaal niets genoteerd.

De directeur/bestuurder is verantwoordelijk voor het beveiligingsbeleid. Het beleid met betrekking tot beveiliging is geïntegreerd in het kwaliteitsbeleid van IJsselgroep. Eén van de eisen van ISO 9001:2015 is het voldoen aan wettelijke regelingen. In dit kader is dat voldoen aan de eisen van AVG. Zo is in het kwaliteitssysteem een proces ingericht en gedocumenteerd voor communicatie over informatiebeveiligingsincidenten en worden Informatiebeveiligingsincidenten benut voor optimalisatie van het informatiebeveiligingsbeleid.

De getroffen beveiligingsmaatregelen worden met het kwaliteitssysteem door de directeur/bestuurder gecheckt en bewaakt; het zorgen voor veiligheid en integriteit met betrekking tot de informatie op zich is de verantwoordelijkheid van de medewerkers die met de gegevens werken.

Medewerkers van IJsselgroep zijn voor alles gebonden aan de integriteits- en geheimhoudingscode die richtlijnen geeft voor nauwgezet en zorgvuldig handelen uitgaand van de belangen van alle betrokkenen. Dit geldt bijvoorbeeld expliciet voor persoonlijke aantekeningen en verslagen van werkzaamheden zoals in annex 1 genoemd en mondeling overgedragen informatie tijdens de werkzaamheden.

Hoewel er afspraken zijn gemaakt over de omgang met (vertrouwelijke) informatie en technische en organisatorische maatregelen zijn getroffen, is IJsselgroep er zich van bewust dat je niet alles kunt regelen of overal afspraken over kunt maken. Medewerkers moeten automatisch 'weten' wat ze wel of niet mogen en kunnen doen met gegevens om de integriteit en de vertrouwelijkheid te waarborgen. Deze houding hoort bij de werkhouding van medewerkers. IJsselgroep stimuleert dit bewustzijn ten aanzien van privacy en informatiebeveiliging en checkt het gedrag jaarlijks onder andere in de audits in het kader van de ISO-certificering.

Het opslaan van de persoonsgegevens kan grofweg opgedeeld worden in twee groepen, die weer onder te verdelen zijn:

- Fysiek
 - In afgesloten (archieff)kasten die alleen toegankelijk zijn voor geautoriseerde medewerkers / sleutelhouders. Het gaat om een beperkte hoeveelheid gegevens: het beleid is gegevens digitaal op te slaan.
 - Specifiek gedrag van medewerkers betreft 'clean desk policy'
- Digitaal
 - In de volgende programma's
 - Profit van AFAS
 - CAAR van JohanICT
 - G-suites van Google
 - Medicare
 - VECOZO
 - Stipter

Met betrokken sub-verwerkers zijn overeenkomsten afgesloten zodat de persoonsgegevens zijn beveiligd, niet veranderd kunnen worden en niet verloren kunnen gaan. Met Google zijn vanuit de Europese Unie afspraken gemaakt omtrent het beveiligen en beheren en opslaan van persoonsgegevens.

Beveiligingsmaatregelen rondom beschikbaarheid

Beschikbaarheid: (informatie)systemen zijn op juiste momenten beschikbaar, zodat medewerkers toegang hebben tot relevante informatie en hun dienstverlening voort kunnen zetten. Niveau belangrijk: de informatie of service mag bijna nooit uitvallen, het bedrijfsproces staat nauwelijks uitval toe. De continuïteit zal snel moeten worden hervat. Schending van dit niveau kan serieuze (in)directe schade toebrengen.

Technische maatregelen

- **Systeembeheer**
IJsselgroep zorgt voor een goede werking van software en netwerkomgeving. Zij heeft haar netwerk op een eigen server, beheerd door sub-verwerker Iselinge Hogeschool.
- **Devices**
Elke medewerker beschikt over voldoende devices en de juiste software om haar werk thuis en op locatie uit te kunnen voeren.

Organisatorische maatregelen

- **Beschikking over relevante stukken voor de uitvoering van werkzaamheden.**
Bij leerlingzorg stuurt de aanvrager de onderzoeksaanvraag naar het kantoor van IJsselgroep. Na een check op volledigheid ontvangt de toegewezen medewerker de aanvraag en plant een onderzoeksdatum. Hiermee garandeert IJsselgroep dat de medewerker over alle relevante informatie beschikt. Bij onderwijsadvies regelt de medewerker zelf de stukken met de betrokkenen van de klant/school.
- **Beschikking over (onderzoeks-)materiaal**
Voor leerlingzorg en onderwijsadvies beschikt IJsselgroep over alle relevante (onderzoeks-) materialen en stuurt voorafgaand aan het werk eventueel noodzakelijk materialen aan de toegewezen medewerker toe.

Beveiligingsmaatregelen rondom integriteit

Integriteit: het waarborgen van de correctheid en volledigheid van informatie en verwerking, waardoor informatie met de werkelijkheid in overeenstemming is en niets ten onrechte is achtergehouden of verdwenen (juistheid, volledigheid en tijdigheid). Niveau absoluut: het bedrijfsproces dat gebruik maakt van deze informatie staat zeer weinig (integriteits-)fouten toe. Bescherming van integriteit is absoluut noodzakelijk. Schending van dit niveau kan serieuze (in)directe schade toebrengen.

Organisatorische maatregel

- **Relevante informatie**
IJsselgroep checkt jaarlijks de offertes en onderzoeksaanvraagformulieren op de relevantie van de vragen om te controleren of zij niet teveel/te weinig gegevens opvraagt om het onderzoek uit te kunnen voeren.
- **PIA**
Voor onderwijsadvies en leerlingzorg zijn de bedrijfsprocessen en de benodigde persoonsgegevens van klanten hiervoor door een Privacy Impact Assessment gecontroleerd op beveiligingseisen.
- **Complete informatieset**
IJsselgroep zorgt ervoor dat voor aanvang van de aangenomen opdracht de relevante informatie van de klant aanwezig is bij de betrokken medewerker van IJsselgroep
- **Dossierbeheer**
IJsselgroep bewaart inzake leerlingzorg de onderzoeksaanvraag, het verslag en eventueel ruwe scores volgens wettelijk afgesproken termijnen (WGBO)4 fysiek en digitaal. Voor onderwijsadvies bewaart IJsselgroep de ondertekende offerte en eventueel relevante documenten alleen digitaal en volgens wettelijk gestelde termijnen.

Maatregel in de vorm van gedrag

- **Onderzoeksverslag:** bij leerlingzorg beschrijft de toegewezen medewerker de resultaten conform de afspraken van de beroepscode voor psychologen.
- **Kwaliteitszorg:** beschrijving en bewaking van de kwaliteit van werkprocessen. IJsselgroep voert jaarlijks een interne en externe audit uit over haar bedrijfsprocessen.

Beveiligingsmaatregelen rondom vertrouwelijkheid

Vertrouwelijkheid: het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn.
Niveau vertrouwelijk: dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde.
Schending van dit niveau kan zeer grote schade toebrengen.

Technische maatregelen

- **Software- en netwerkbeveiliging**
IJsselgroep werkt met een eigen netwerkomgeving en bedrijfsemail dat beveiligd is en afgeschermd met een wachtwoord, dat aan hoge eisen moet voldoen. Er zijn maatregelen geïmplementeerd tegen misbruik en aanvallen:
 - Antivirusprogramma's
 - Firewall
 - Automatische softwareupdates
 - Automatische back-ups
 - Afdankte apparatuur wordt zorgvuldig geschoond
 - Fysieke gegevens worden jaarlijks conform wettelijke bewaartermijnen door een professionele papiervernietiger vernietigd.
 - Medewerkers beveiligen alle devices (laptops, telefoons, tablets) die zij gebruiken voor onderwijsadvies en leerlingzorg met een wachtwoord en (eventueel) encryptie.
- **Autorisatiebeleid**
Het autorisatiebeleid zorgt ervoor dat medewerkers alleen toegang hebben tot persoonsgegevens voor zover dat nodig is om hun werkzaamheden uit te voeren.
Toegankelijkheid van digitale aanvragen, onderzoeksgegevens en verslag alleen door betrokken behandelaren en het bedrijfsbureau. Dit is ingericht op in alle administratiesystemen van IJsselgroep.
- **Fysieke persoonsgegevens**
Fysiek bewaarde persoonsgegevens worden bewaard in een afgesloten kast gedurende de wettelijke bewaartermijn en zijn alleen toegankelijk voor geautoriseerde medewerkers.
- **Plaats/land van opslag en verwerking van persoonsgegevens**
Bewerker zal geen persoonsgegevens van Verantwoordelijke doorgeven aan (een partij gevestigd in) een land dat door de Europese Unie niet is aangemerkt als een land waar privacy adequaat is beschermd, tenzij Bewerker met de betreffende partij een bewerkersovereenkomst heeft gesloten waarbij de relevante door de Europese Commissie beschikbaar gestelde modelclausules zijn opgenomen, of in het geval van verwerking in de Verenigde Staten in ieder geval wordt voldaan aan de vereisten van het EU-US Privacy Shield. Voor de meerderheid van de persoonsgegevens geldt dat ze binnen de Europese ruimte worden opgeslagen. IJsselgroep werkt tevens met Google for Education (G-suites) software. Voor deze gegevens geldt dat Google voldoet aan de vereisten van het EU-US Privacy Shield.

Organisatorische maatregelen

- **Geheimhoudingsverklaring**
Medewerkers hebben een geheimhoudingsplicht, vastgelegd in de cao onderwijsadviesbureaus.
Subverwerkers hebben een geheimhoudingsplicht, vastgelegd in een overeenkomst met IJsselgroep.
- **Protocol melding datalekken**
IJsselgroep beschikt over een wettelijk verplicht protocol melding datalekken. Bij elk persoonsgegeven dat gelekt wordt treedt dit protocol in werking.
- **Inhuur derden en sub-verwerkers**
IJsselgroep maakt soms gebruik van derden en sub-verwerkers. Hiermee sluit zij een (sub)verwerkersovereenkomst die voldoet aan de wettelijke normen van de AVG.

Maatregelen in de vorm van gedrag

- **Uitwisseling van gegevens**
Fysieke post wordt verstuurd aan de ouders en/of de ib'er van de school naar het door hen zelf opgegeven postadres door de medewerker en/of het bedrijfsbureau en is beschermd met het juridische briefgeheim.
Digitale post wordt aan ouders en/of de ib'er van de school verstrekt op het door hen zelf opgegeven mailadres.