ANNEX 2

BEVEILIGINGSMAATREGELEN

De beveiligingsmaatregelen getroffen door de Verwerker:

Omschrijving van de technische en organisatorische beveiligingsmaatregelen die door de Verwerker zijn geïmplementeerd.

Zoals opgenomen in artikel 4 van deze overeenkomst treft Verwerker passende technische en organisatorische maatregelen - rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging van deze maatregelen - om de Persoonsgegevens te beschermen tegen verlies, onrechtmatige verwerking of onrechtmatige toegang. De getroffen maatregelen zijn opgenomen in deze Annex 2 en worden aangevuld of gewijzigd indien dat nodig is.

A. Algemene informatie over getroffen beveiligingsmaatregelen.

Stichting OnderwijsAdvies hecht veel belang aan het juiste gebruik van (persoons)gegevens. Daarvoor is beleid geformuleerd dat actief wordt uitgedragen en zijn gegevensstromen in kaart gebracht, zodat maatregelen kunnen worden genomen om 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 directie is verantwoordelijk voor het beveiligingsbeleid.

Het beleid met betrekking tot beveiliging is geïntegreerd in het kwaliteitsbeleid van Stichting OnderwijsAdvies. Eén van de eisen van ISO 9001: 2015 is het voldoen aan wettelijke regelingen. In dit kader is voldaan aan de eisen van WBP en 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 directie gecheckt en bewaakt; het zorgen voor veiligheid en integriteit met betrekking tot de informatie op zich is de verantwoordelijkheid van de betreffende managers en de medewerkers die met de gegevens werken.

Werken aan kwaliteit is geïntegreerd in het handelen van alle dag.

Medewerkers van Stichting OnderwijsAdvies zijn voor alles gebonden aan de integriteits- en geheimhoudingscode die richtlijnen geeft voor nauwgezet en zorgvuldig handelen uitgaande 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 Stichting OnderwijsAdvies 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 'risico bewuste houding' hoort 'bij de bagage' van medewerkers. Stichting OnderwijsAdvies 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.

Overzicht maatregelen

- Netwerk is voorzien van hardware- en softwarematige firewalls waarbij enkel de noodzakelijke poorten zijn opengesteld.
- Mappen, bestanden en applicaties met gevoelige gegevens zijn afgeschermd met wachtwoorden.
- Er is fysieke toegangsbeperking tot de serverruimtes.
- Afgesloten (archief)kasten die alleen toegankelijk zijn voor geautoriseerde medewerkers/ sleutelhouders. Het gaat om een beperkte hoeveelheid gegevens: het beleid is gegevens digitaal op te slaan.
- Mobiele telefoons zijn voorzien van pincode en mogelijkheid tot wissen op afstand.
- Pc's met een TPM en Windows 10 worden versleuteld met Bitlocker.
- Gedetailleerdere informatie is te vinden in het Beleidsplan Kantoorautomatisering.

Audits/Derden-verklaringen

- ISO 9001: 2008.
- Accountantsverklaring.
- Profit & Care 4/4 Consult: ISO 27001.

B. Maatregelen om te zorgen dat uitsluitend bevoegd personeel toegang heeft tot de Persoonsgegevens.

Autorisaties

- Map- en applicatierechten zijn ingesteld op basis van functie/bevoegdheden.
- Eisen aan de medewerker:
    - de medewerker is verantwoordelijk voor het gebruik van de software en de communicatie van de gegevens van de kinderen aan hun ouders/verzorgers.
    - vanuit zijn verantwoordelijkheid zorgt Stichting OnderwijsAdvies voor een goede werking van de software en informatie die nodig is om dit te waarborgen.

- Geheimhoudingsverklaring:
    - met medewerkers (zowel intern als extern) worden geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt.
    - van subverwerkers wordt verwacht dat zij een geheimhoudingsverklaring hebben getekend conform hun eigen (vereiste) beveiligingsbeleid. Dit beveiligingsbeleid wordt/is tevoren gecontroleerd en wordt jaarlijks getoetst.

Toelichting en overzicht maatregelen

- Gedetailleerdere informatie in het Beleidsplan Kantoorautomatisering.

C. Maatregelen om de Persoonsgegevens te beschermen tegen verlies of wijziging en tegen onbevoegde of onrechtmatige verwerking, toegang of openbaarmaking.

Toelichting en overzicht maatregelen

- Alle medewerkers hebben een geheimhoudingsclausule ondertekend.

Beveiliging systemen voor opslag

- Dataopslag is voorzien van schijven in RAID 1 of 5 opstelling.
- Servers maken gebruik van ‘shadowcopies’.
- Back-ups op tape of in de Cloud (tapes worden off site bewaard).

Beveiliging verbindingen

- Voor verbinding tussen de locaties wordt gebruik gemaakt van VPN’s.
- Gevoelige sites/webapplicaties gebruiken HTTPS.
- Systemen zijn voorzien van firewalls waarbij alleen de noodzakelijk poorten opengesteld zijn.
- Mailverbindingen gebruiken TLS (waar mogelijk).
- Gedetailleerdere informatie in het Beleidsplan Kantoorautomatisering.
    - Op lokale werkstations en servers worden passende maatregelen genomen om te voorkomen dat kwaadaardige programmatuur of functionaliteit wordt geïnstalleerd. Op wachtwoorden worden cryptografische maatregelen (hashing) toegepast, van een kwaliteit die in de industrie over het algemeen als veilig wordt beschouwd, om deze gegevens veilig op te slaan. Er wordt voor inlogprocessen gebruik gemaakt van beveiligde/versleutelde verbindingen waaronder https.
    - Wachtwoorden worden niet met reversible encryption opgeslagen en kunnen dus nooit terug gelezen worden.
    - De uitwisseling van persoonsgegevens, ook via e-mail, tussen de onderwijsinstelling en Stichting OnderwijsAdvies vindt beveiligd, versleuteld en/of in een met een wachtwoord versleutelde pdf plaats.
    - Afgedankte apparatuur wordt zorgvuldig geschoond (in het geval van vestiging Zoetermeer, Leiden en Gouda door Stichting Ecoware te Zoetermeer). Van het schonen wordt per e-mail een rapport verstrekt.
    - Persoonlijke gegevens op papier worden in afgesloten containers afgevoerd en vernietigd.
    - Overgebleven tapes en harddisk worden afgevoerd en vernietigd door een gespecialiseerd bedrijf.

Plaats/land van opslag en verwerking van de Persoonsgegevens

Verwerker zal geen persoonsgegevens van Verwerkingsverantwoordelijke 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 Verwerkersovereenkomst 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-U.S. Privacy Shield.

Voor de meerderheid van de persoonsgegevens geldt dat ze binnen de Europese ruimte worden opgeslagen. Stichting OnderwijsAdvies werkt ook met *Office365.* Voor deze gegevens geldt dat ze in de Cloud worden opgeslagen waarbij geldt dat Microsoft voldoet aan de vereisten van het EU-US Privacy Shield.

D. Maatregelen incidentenbeheer

Ingeval van incidenten m.b.t. het beheer van de data wordt gehandeld volgens het “Brancheformat documentatie van gegevens bij Datalek” en de voorschriften van de autoriteit persoonsgegevens.

- Gedragscode en protocol datalekken.
- Contactpersoon bij datalekken: de heer T.M. van der Meer, 079-3295600, m.vdmeer@onderwijsadvies.nl.