Stichting OPO Borger–Odoorn
Openbaar Primair Onderwijs

Informatiebeveiliging en privacy Beleid

Informatiebeveiligings- en Privacy Beleid

Bron
Kennisnet

Bewerkt door:
Stichting OPO Borger-Odoorn

Versie	Status	Datum	Auteur	Omschrijving
1.0	Definitief	November 2020	A. Sueters	

Vastgesteld door Stichting OPO Borger-Odoorn

Versie	Datum	Naam	Functie
1.0	November 2020	J. Drok	Directeur Bestuurder

1 Inleiding

Het belang van informatiebeveiliging en privacy
Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ICT. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ICT en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van **informatiebeveiliging en privacy** (afgekort tot IBP) in een IBP-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

Onder **informatiebeveiliging** wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden.
Informatiebeveiliging richt zich op de volgende aspecten:

- Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- Integriteit: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot ongewenste risico's in het onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden.
Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van **verwerking**:
Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

Vervlechting informatiebeveiliging en privacy

Informatiebeveiliging is een belangrijke voorwaarde voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één proces. Dit beleid vormt de basis op informatiebeveiliging en privacy binnen Stichting OPO Borger-Odoorn te regelen en vormt de kapstok voor de onderliggende afspraken en procedures. Dit document is een invulling van artikel 24 lid 2 van de AVG.

2 Doel en reikwijdte

2.1 Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan Stichting OPO Borger-Odoorn

persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/ verzorgers, medewerkers en externe relaties.
- Zorgvuldig beschermen van de privacy van alle betrokkenen van wie Stichting OPO Borger-Odoorn persoonsgegevens verwerkt of laat verwerken, en in de lijn met de AVG.
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het informatiebeveiligings- en privacy beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene (o.a. medewerkers, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en Stichting OPO Borger-Odoorn voldoet aan relevante wet- en regelgeving.

2.2 Reikwijdte

Het informatiebeveiligings- en privacy beleid binnen Stichting OPO Borger-Odoorn geldt voor alle medewerkers, leerlingen, ouders/ verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/ outsourcing). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.

Het Informatiebeveiligings- en privacy beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Stichting OPO Borger-Odoorn waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan Stichting OPO Borger-Odoorn persoonsgegevens verwerkt.

Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Stichting OPO Borger-Odoorn. Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de school kan worden aangesproken. (b.v. uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites en of social media).

Het Informatiebeveiligings- en privacy beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/ systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van Stichting OPO Borger-Odoorn evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het Informatiebeveiligings- en privacy beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Informatiebeveiligings- en privacy beleid heeft binnen Stichting OPO Borger-Odoorn raakvlakken met:

- *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen.
- *Personeels- en organisatiebeleid;* met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties
- *IT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ICT en (digitale) leermiddelen
- *Medezeggenschap (MR) en gemeenschappelijke medezeggenschap (GMR)* van ouders/ verzorgers en medewerkers.

3 Uitgangpunten privacy beleid

Stichting OPO Borger-Odoorn hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het schoolbestuur van Stichting OPO Borger-Odoorn neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.

2. Stichting OPO Borger-Odoorn voldoet aan alle relevante wet- en regelgeving.

3. Bij Stichting OPO Borger-Odoorn is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van Stichting OPO Borger-Odoorn om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/ haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen ten alle tijden hun toestemming herzien.

4. Stichting OPO Borger-Odoorn zal alle betrokkenen helder en actief informeren over de verwerkingen van de hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering.

5. Stichting OPO Borger-Odoorn legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Stichting OPO Borger-Odoorn voldoet hiermee aan de documentatieplicht.

6. Binnen Stichting OPO Borger-Odoorn is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.

7. Stichting OPO Borger-Odoorn is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.

8. Stichting OPO Borger-Odoorn classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de tenemen maatregelen.

9. Stichting OPO Borger-Odoorn sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.

10. Stichting OPO Borger-Odoorn verwacht van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/ of imagoverlies. Stichting OPO Borger-Odoorn heeft hiervoor een

gedragscode geformuleerd, vastgesteld en geïmplementeerd.

11. Informatiebeveiliging en privacy is bij Stichting OPO Borger-Odoorn een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

12. Stichting OPO Borger-Odoorn kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vóóraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.

13. Stichting OPO Borger-Odoorn neemt passende technische (beveiligings-)maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren.

14. Stichting OPO Borger-Odoorn zal alle beveiligingsincidenten vastleggen en datalekken volgens het protocol beveiligingsincidenten en datalekken afgehandeld.

4 Wettelijke kader

Stichting OPO Borger-Odoorn is wettelijk verplicht om zorgvuldig om te gaan met persoonsgegevens. Het bescherming van de persoonsgegevens is een grondrecht, die opgenomen is in de Grondwet (art. 10).

Op 25 mei 2018 is de Algemene Verordening gegevensbescherming (AVG) van kracht. Deze Europese privacy verordening vervangt de bestaande Wet bescherming persoonsgegevens (Wbp).
De intreding van de AVG brengt een vernieuwd en aangescherpt juridisch kader voor de bescherming van persoonsgegevens die beter aansluit bij de hedendaagse praktijk. De nieuwe wetgeving zorgt, ten opzichte van de vorige privacy wetgeving, voor versterking en uitbreiding van de privacy rechten, meer verantwoordelijkheden voor de organisaties en een Europese wetgeving voor privacy. AVG biedt ook de ruimte om specifieke bepalingen en uitzonderingen op nationaal niveau te reguleren. Deze bepalingen en uitzonderingen zijn uitgewerkt in de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) en de andere relevante wet- en regelgeving die van toepassing zijn voor, in dit geval, het onderwijs sector.

4.1 Relevante wet- en regelgeving

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra
- Wet goed onderwijs en goed bestuur PO/VO
- Wet onderwijstoezicht
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)
- Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

4.2 Beginselen met betrekking tot het verwerken van persoonsgegevens:

- De verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn.

- De verwerking moet voor een gerechtvaardigd doel zijn oftewel er moet sprake zijn van een doelbinding.
- De verwerking van persoonsgegevens moet beperkt zijn tot wat noodzakelijk is voor het doel van de verwerking: minimale gegevensverwerking.
- Persoonsgegevens mogen niet langer worden bewaard dan voor de doeleinden waar zij voor worden verwerkt noodzakelijk is: opslagbeperking.
- De persoonsgegevens moeten juist zij en zo nodig worden geactualiseerd.
- De persoonsgegevens moeten dusdanig beveiligd zijn dat de integriteit en de vertrouwelijkheid worden gewaarborgd.
- De verantwoordelijke kan de naleving van bovenstaande beginselen aantonen: verantwoordingsplicht.

4.3 Verplichtingen die voortvloeien uit de AVG:

- Het aanwijzen van een Functionaris Gegevensbescherming.
- Meldingen doen bij een datalek (indien van toepassing) aan de externe toezichthouder (Autoriteit Persoonsgegevens).
- Mededelingen doen bij een inbreuk in verband met persoonsgegevens (indien van toepassing) aan betrokkenen.
- In kennis stellen aan betrokkenen over het gebruik van persoonsgegevens of bij bijvoorbeeld bij het doorgeven van persoonsgegevens.
- Het doen van gegevenseffect beoordelingen (DPIA) ten aanzien van gegevensbescherming.
- Voorafgaande raadpleging van de externe toezichthouder bij de combinatie risicovolle verwerkingen en het niet kunnen treffen van gegevensbeschermingsmaatregelen.
- Bijhouden van een register van verwerkingsactiviteiten (dataregister).
- Nemen en onderhouden van passende technische en organisatorische gegevensbeschermingsmaatregelen.

4.4 Basisregels bij het omgaan met persoonsgegevens

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake verwerking persoonsgegevens (art.5 AVG) leidend. Deze zijn samengevat in de **vijf vuistregels** met betrekking tot de omgang met persoonsgegevens te weten:

1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld.
   Bijvoorbeeld: Bij de inschrijving van een kind moet de school duidelijk aangeven welke gegevens worden verwerkt en waarvoor. Elk school is wettelijk verplicht om voor een vastgestelde datum gegevens van de kinderen aan DUO (Dienst Uitvoering Onderwijs) te verstrekken voor de bekostiging.

   Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
   Bijvoorbeeld: ouders hebben hun telefoonnummer doorgegeven aan de school zodat de school hun kan bereiken bijvoorbeeld in geval van een noodsituatie. De school mag de telefoonnummer niet gebruiken om de ouders uit te nodigen voor een informatie avond van de gemeente voor bijvoorbeeld de opknapbeurt van de wijk waar de school zich bevindt.

2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen.
   a. Ik heb **toestemming** van leerling of ouders/ verzorgers

Bijvoorbeeld: voor het gebruik van foto's of beeldmateriaal van leerlingen hebben ouders vooraf toestemming voor gegeven (middels het formulier Toestemming publicatie foto's en video's).

b. De gegevens zijn nodig voor de **uitvoering van een overeenkomst**
Bijvoorbeeld: het inschrijf formulier is een overeenkomst tussen ouders/ leerling en school.

c. Het verwerken van deze gegevens is **wettelijk verplicht**
Bijvoorbeeld: doorgeven van leerling informatie aan de Ministerie van Onderwijs en Cultuur is één van de wettelijke verplichtingen van een onderwijsinstelling.

d. De verwerking van gegevens is nodig voor het **uitvoeren van onze publiekrechtelijke taak**
Bijvoorbeeld: de opgedragen publiekrechtelijke taak van een school is het geven van onderwijs. Daarvoor is het noodzakelijk om gegevens van leerlingen te verwer-ken.

e. Er is een **gerechtvaardigd belang** dat ik kan uitleggen aan (de ouders van) de leer-lingen.
Bijvoorbeeld: onder strikte voorwaarden en met oog op de privacy van betrokke-nen worden op sommige scholen cameratoezicht gebruikt.

f. De verwerking van persoonsgegevens is noodzakelijk om een ernstige bedreiging van de gezondheid van betrokkenen te beperken: **vitale belangen**
Bijvoorbeeld: tijdens schooltijd valt een leerling.

3. **Dataminimalisatie**: bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding staan tot het doel (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (subsidiar). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.

4. **Transparantie**: de school legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde Informatiebeveiligings-en privacy beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Tevens kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.

5. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

5 Ondersteunende richtlijnen en procedures

5.1 Beleidsstukken, procedures en protocollen

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Een overzicht van de diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen zijn opgenomen in de bijlage. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

5.2 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hier een belangrijke factor. Daarom wordt het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers en leerlingen. Verhoging van het informatiebeveiligings- en privacy bewustzijn is een gezamenlijke verantwoordelijkheid van de FG met het bestuur als eindverantwoordelijke.

5.3 Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de betrouwbaarheidsaspecten die van belang zijn.

5.4 Privacy bij design en privacy bij default

Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen wordt het principe van privacy bij design en privacy bij default toegepast. In de praktijk betekent privacy bij design dat vóóraf wordt gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden. Vanaf de start van nieuwe (ICT)projecten wordt rekening gehouden met informatiebeveiliging en privacy.
Privacy bij default wordt toegepast om zo vriendelijk mogelijk privacy instellingen te kunnen garanderen. Privacy bij default houdt in dat bijvoorbeeld bij een ouder communicatiemiddel worden de instellingen zo ingezet dat er zo min mogelijk al aangevinkt is.

5.5 Incidenten en datalekken

Alle medewerkers, die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister. Alle (beveiligings)incidenten kunnen worden gemeld bij privacy@opoborger-odoorn.nl.
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

5.6 Convenanten en verwerkersovereenkomsten

Scholen maken gebruik van digitale leermiddelen en leerling administratiesystemen. Wanneer er een externe partij in opdracht van de school persoonsgegevens gaat verwerken, moet er afgestemd worden op welke manier deze partijen dienen om te gaan met de gegevens die zij in onze opdracht verwerken. In convenanten en verwerkersovereenkomsten worden afspraken gemaakt over het verwerking van persoonsgegevens.

Bij het gebruik maken van een externe partij is het van belang om na te denken over de rollen en verantwoordelijkheden met betrekking tot de verwerking. Bijvoorbeeld: wie toegang mag krijgen tot de gegevens en welke gegevens noodzakelijk zijn om hun taak te kunnen uitvoeren, welke maatregelen de externe partij neemt om de gegevens te beschermen.

5.7 Register van verwerkingsactiviteiten

Op basis van artikel 30 van de AVG is Stichting OPO Borger-Odoorn verplicht om alle verwerkingen (Stichting OPO Borger-Odoorn als verantwoordelijke of verwerker) op te nemen in een register van verwerkingsactiviteiten. Alle nieuwe verwerkingen en mutaties worden door de verantwoordelijke (school directeur) aan de FG doorgegeven. De FG beoordeeld de verwerking en neemt het op in het dataregister.

In het dataregister worden naast het opnemen van de verwerking ook informatie over het doel waarvoor de gegevens worden verwerkt, het opslag van de gegevens (in welke systemen worden de gegevens opgeslagen), hoe lang mogen de gegevens bewaard worden en wat er na die termijnen mee gebeurt, met wie worden de gegevens gedeeld en welke technische maatregelen worden genomen om de gegevens te beveiligen.

5.8 DPIA (Gegevensbeschermingseffect-beoordeling)

Wanner een verwerking en in het bijzonder wanneer er een verwerking waarbij nieuwe technologieën worden gebruikt een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen wordt vóór de verwerking een beoordeling uitgevoerd van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.
De uitvoering van een gegevensbeschermingseffect-beoordeling, ook wel **D**ata **P**rotection **I**mpact **A**ssesments (DPIA) genoemd, zorgt dat de risico's van een verwerking in kaart worden gebracht en door praktische, organisatorische en technische maatregelen deze risico's worden beheerst.

De Autoriteit Persoonsgegevens (AP) heeft een definitieve lijst vastgesteld van verwerkingen van persoonsgegevens waarvoor een **D**ata **P**rotection **I**mpact **A**ssessment (DPIA) nodig is. Deze lijst kan je vinden op de website van de Autoriteit persoonsgegevens .

5.9 Planning en controle

Dit Informatiebeveiligings- en privacy beleidwordt minimaal elke twee jaar getoetst en bijgesteld door het bestuur. Hierbij wordt rekening gehouden met:

- De status van de informatiebeveiliging als geheel (beleid, organisatie, risico's)
- De actuele geinventariseerde risico's
- De effectiviteit van de genomen maatregelen en aantoonbare werking daarvan

Daarnaast doet Stichting OPO Borger-Odoorn een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen.

5.10 Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera.
Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de het bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het bestuur vast te stellen reglement.

Mocht de naleving van dit beleid ernstig tekort schieten, dan kan Stichting OPO Borger-Odoorn de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

5.11 Logging en monitoring

Logging en monitoring door de IT-afdeling zorgt er voor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in- uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk.

6 Organisatie – rollen en verantwoordelijkheden

De organisatie van informatiebeveiliging en privacy gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen bij Stichting OPO Borger-Odoorn.

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	Bevoegd gezag: Directeur bestuurder	• Eindverantwoordelijk • Privacy-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking Privacy beleid op basis van rapportages • Privacy organisatie inrichten • FG vooraf informeren over nieuwe verwerkingen of verwerkingen waarin nieuwe technologie wordt toegepast, of verwerkingen waarin de risico voor betrokkenen hoog is.	• Informatiebeveiligings- en privacy beleid • Baseline / basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen • FG informeren over nieuwe verwerkingen van persoonsgegevens en technologieën die gebruikt worden waarbij persoonsgegevens worden verwerkt
	Privacy officer (PO) (de persoon die inhoudelijk verantwoordelijk is voor Privacy)	• Inhoudelijk verantwoordelijk voor Privacy • Privacy-planning en controle • Adviseert bestuur/CvB/directie over Privacy • Voorbereiden uitvoeren Privacy-beleid, Classificatie/risicoanalyse • Hanteren Privacy normen en wijze van toetsen • Evalueren Privacy-beleid en maatregelen • Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze • Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen • Incidentafhandeling (registreren en evalueren).	Privacy processen, richtlijnen en procedures, waaronder: • Activiteitenkalender • Protocol beveiligingsincidenten en datalekken • Verwerkersovereenkomsten regelen • Brief toestemming gebruik beeldmateriaal • Opstellen informatie documentatie richting leerlingen, ouders/ verzorgers • Security awareness activiteiten • Sociale media reglement • Gedragscode ICT en internetgebruik • Gedragscode medewerkers en leerlingen • Nieuwe verwerkingen opnemen in het verwerkingsregister
	Functionaris Gegevensbescherming (FG)	• De verwerkingsverantwoordelijke en de werknemers die verwerken, informeren adviseren over hun verplichtingen uit hoofde van de AVG en an-	• Privacyreglement, • Protocol beveiligingsincidenten en datalekken • Inrichten meldpunt datalekken

		dere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen • Toezien op naleving van de AVG en van het beleid van de verwerkingsverantwoordelijke met betrekking tot de bescherming van persoonsgegevens met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits • Desgevraagd advies verstrekken met betrekking tot de gegevensbeschermingseffectbeoordeling (DPIA) en toezien op de uitvoering daarvan in overeenstemming met artikel 35 van de AVG • Met de Autoriteit Persoonsgegevens samenwerken • Optreden als contactpunt voor de Autoriteit Persoonsgegevens inzake met verwerking verband houdende aangelegenheden, met inbegrip van de in artikel 36 van de AVG bedoelde voorafgaande raadpleging, en, waar passend, overleg plegen over enige andere aangelegenheid • Toezien op melden, mededelen van inbreuken in verband met persoonsgegevens in overeenstemming is met artikel 33 en 34 van de AVG • Toezien dat aan verzoeken inzake rechten van betrokkenen wordt voldaan	
	Domeinverantwoordelijke/ Proceseigenaren Waaronder o.a.: ICT, HRM / P&O, facilitair, onderwijs, financiën, inkoop en administratie	• **Classificatie / risicoanalyse** in samenwerking met de Privacy Officer • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door bestuur/CvB/directie • Samen met functioneel beheer en ICT beheer er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. • Samen met functioneel beheer en ICT beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren. • Privacy officer vooraf informeren over nieuwe verwerkingen of verwerkingen waarin nieuwe technologie wordt toegepast, of verwerkingen waarin de risico voor betrokkenen hoog is.	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst); input dataregister • Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk • FG/ PO informeren over nieuwe verwerkingen van persoonsgegevens en technologieën die gebruikt worden waarbij persoonsgegevens worden verwerkt

Uitvoerend (operationeel)	Functioneel en/of applicatie beheerder Medewerker Dagelijkse leiding / leidinggevende / school directeur	• Uitvoeren taken conform gegeven richtlijnen en procedures. • Verantwoordelijk omgaan met Privacy bij hun dagelijkse werkzaamheden. • Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan. • Toezien op de naleving van het Privacy beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Voorbeeldfunctie met positieve en actieve houding t.a.v. Privacy beleid. • Implementeren Privacy maatregelen. • Periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.; • Rapporteren voortgang m.b.t. doelstellingen Privacy beleid aan bestuur. • Privacy officer vooraf informeren over nieuwe verwerkingen of verwerkingen waarin nieuwe technologie wordt toegepast, of verwerkingen waarin de risico voor betrokkenen hoog is.	Communiceren, informeren en toezien op naleving van o.a.: • Privacy in het algemeen • Regels passend onderwijs • Hoe omgaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken • FG/ PO informeren over nieuwe verwerkingen van persoonsgegevens en technologieën die gebruikt worden waarbij persoonsgegevens worden verwerkt

Bijlage: Ondersteunende richtlijnen en procedures

Deze bijlage bevat een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Een aantal zijn vanuit de Algemene Verordening Gegevensbescherming verplicht.

- Privacyreglement Stichting OPO Borger-Odoorn – *beschrijving van de afspraken rond de verwerking van persoonsgegevens binnen Stichting OPO Borger-Odoorn*
- Procedure Verzoek rechten van Betrokkenen – *beschrijving van de procedure rond het uitoefenen van de rechten van betrokkenen conform AVG*
- Formulier verzoek privacyrechten van Betrokkenen
- Protocol Informatiebeveiligingsincidenten en datalekken – *beschrijving van de procedure bij het melden van een informatiebeveiligingsincident/ datalek*
- Gedragscode veilig gebruik van ICT-middelen – *beschrijving van de afspraken bij het gebruik van ICT-middelen*
- Social media binnen Stichting OPO Borger-Odoorn – *beschrijving van de afspraken bij het gebruik van social media binnen Stichting OPO Borger-Odoorn*
- Toestemmingformulier gebruik beeldmateriaal
- Procedure voor bewaartermijnen en verwijderen van gegevens – *beschrijving van de afspraken en procedures bij het bewaren en vernietigen van persoonsgegevens*
- Responsible disclosure – *beschrijving van de afspraken bij het ontdekken van een beveiligingsincident door een externe*

Naast bovenstaande beleidsstukken, procedures en protocollen maakt Stichting OPO Borger-Odoorn gebruik van de volgende "open" documenten.

- Registratie beveiligingsincidenten en datalekken – *hierbij worden de informatiebeveiligingsincidenten en datalekken bijgehouden*
- Verwerkingsregister – *hierbij worden alle verwerkingen binnen Stichting OPO Borger-Odoorn, persoonsgegevens, bewaartermijnen etc. bijgehouden*
- Verwerkersovereenkomsten – *overeenkomsten waarin afspraken met leveranciers en externe verwerkers van Stichting OPO Borger-Odoorn worden bijgehouden*
- Procedure gegevensbeschermingseffectbeoordeling (DPIA) – *risicoanalyse procedure bij door in de wet aangegeven nieuw en specifieke verwerkingen*