SAMENWERKINGSVERBAND
VO ZAANSTREEK

Informatiebeveiligings- en privacybeleid (IBP) voor het Samenwerkingsverband VO Zaanstreek

Vastgesteld door directeur-bestuurder	13 oktober 2023
Goedgekeurd door Raad van Toezicht	12 oktober 2023
Instemming MR-p	03 oktober 2023

Inhoud

Voorwoord

Digitalisering in de maatschappij leidt tot toenemende beschikbaarheid van data en potentieel dus tot nieuwe of rijkere informatie. Digitalisering speelt ook een grote rol binnen het onderwijs, datasturing en informatisering maken het mogelijk om steeds beter samen te werken.

Digitalisering brengt ook risico's met zich mee. Het leidt tot vraagstukken rondom het verzamelen van data en de verschillende vormen van classificatie daarbinnen. Denk daarbij in het bijzonder aan persoonsgegevens. Met welk doel worden ze verzameld, wie beslist hierover, wie heeft ervoor getekend? En indien je met de juiste doelbinding beschikt over data hoe ga je er dan qua beveiliging mee om, zodat je voorkomt dat ze in verkeerde handen kunnen vallen.

Het samenwerkingsverband ondersteunt scholen bij het aanbieden van passend onderwijs. Omdat we daarbij met gevoelige persoonsgegevens omgaan, moet informatiebeveiliging en privacy voor ons natuurlijk op orde zijn. In dit document laten wij zien aan iedereen met wie wij samenwerken, intern en extern, hoe wij dat georganiseerd hebben.

Voor het samenwerkingsverband zijn informatiebeveiliging en privacy onlosmakelijk met elkaar verbonden en integraal onderdeel van beleid, processen en uitvoering. Voor de verwerking van persoonsgegevens kent het samenwerkingsverband een tweetal verwerkers:

- OVO Zaanstad. Het samenwerkingsverband neemt van deze organisatie financiële, personele, facilitaire en ICT-dienstverlening af;
- Indigo voor de verwerking van leerlinggegevens.

Met beide organisaties zijn verwerkersovereenkomsten overeengekomen.

Lydie van de Laar
Directeur-bestuurder SVZ

1. Het belang van informatiebeveiliging en privacy

Uitwisselen van persoonsgegevens is onderdeel van het dagelijks werk in het samenwerkingsverband. Hierbij hebben we te maken met een groot aantal mogelijke bedreigingen. Alle systemen die we gebruiken en gegevens die we bewaren en verwerken, kunnen worden bedreigd door bijvoorbeeld een aanval, een vergissing of de natuur (zoals een overstroming of brand).

Datalekken, incorrecte gegevens of diensten die niet beschikbaar zijn - in het ergste geval schaden deze incidenten onze bedrijfsvoering en daarmee het vertrouwen. Daarom zijn de continuïteit van onze dienstverlening en privacybescherming van groot belang. Ook treffen we gericht maatregelen om mogelijke risico's tot een aanvaardbaar niveau te reduceren.

Het bestuur doet daarom een beroep op iedereen die betrokken is bij de activiteiten van het Samenwerkingsverband waaronder de verwerkers, vanuit een gemeenschappelijke visie en wil, de verwerking van (persoons)gegevens correct te laten verlopen.

Dit beleid gaat dieper in op de bescherming van ict en in het bijzonder persoonsgegevens. Het dient als norm en leidraad voor alle informatieverwerking en biedt een uitgangspunt voor audit en controle.

Dit beleid biedt elke belanghebbende – medewerker, ouder, school of relatie – inzage in de manier waarop we omgaan met persoonsgegevens.

1.1. De scope van het informatiebeveiligings- en privacybeleid

Het informatiebeveiligings- en privacybeleid is van toepassing op alle informatieverwerking binnen en namens het samenwerkingsverband.

Het beleid is van toepassing op onze eigen medewerkers, tijdelijk personeel en op personeel dat, op basis van een verwerkersovereenkomst, door derden wordt ingezet om diensten te verlenen aan of namens onze organisatie.

1.2. Het doel van informatiebeveiliging en privacy

Het Informatiebeveiligings- en privacybeleid heeft de volgende doelen:

- Het waarborgen van de continuïteit van de dienstverlening;
- Het beschermen van de privacy van eenieder van wie het samenwerkingsverband persoonsgegevens verwerkt;
- Het voorkomen en zo goed mogelijk afhandelen van incidenten;
- Het minimaliseren van de eventuele gevolgen van incidenten.

Bij het realiseren van deze doelen bewaakt het samenwerkingsverband de balans tussen werkbaarheid – in de meest brede zin van het woord – en informatiebeveiliging en privacy.

2. Het beleid

Het beleid bestaat uit keuzes die het samenwerkingsverband maakt om de doelen rond informatiebeveiliging en privacy te bereiken.

2.1. Voorbeeldrol

Het samenwerkingsverband heeft een voorbeeldrol in de onderwijsketen en communiceert helder en actief over informatiebeveiliging en privacy. Alle medewerkers en diensten van het samenwerkingsverband dienen voorbeeldig te zijn wat betreft informatiebeveiliging en privacy.

2.2. Wet- en regelgeving

Het samenwerkingsverband houdt zich aan alle relevante wet- en regelgeving

Twee regels vormen daarbij de basis:

- De directeur-bestuurder van het samenwerkingsverband is als verwerkingsverantwoordelijke eindverantwoordelijk voor de bescherming van persoonsgegevens.
- Het samenwerkingsverband hanteert passende technische en organisatorische maatregelen voor het beschermen van diensten en in het bijzonder persoonsgegevens en verlangt dit ook van de verwerkers.

2.3. IBP is overal in verweven

Het samenwerkingsverband beschouwt informatiebeveiliging en privacy als onlosmakelijk met elkaar verbonden en als belangrijk onderdeel van het beleid, de processen en de uitvoering van diensten. Daar waar mogelijk wordt informatiebeveiliging en privacy opgenomen in bestaande processen.

2.4. IBP is de verantwoordelijkheid van iedereen

Omdat iedereen binnen en rondom het samenwerkingsverband bijdraagt aan informatiebeveiliging en privacy, zijn de rollen en verantwoordelijkheden rondom informatiebeveiliging en privacy duidelijk vastgelegd.

2.5. IBP is een continu proces

Informatiebeveiliging en privacy is in het samenwerkingsverband een continu proces. Hierbij is het proces voor informatiebeveiliging doorlopend en cyclisch. Dat betekent dat het samenwerkingsverband jaarlijks de organisatie als geheel evalueert, controleert en verbetert. Nieuwe ontwikkelingen of incidenten, binnen en buiten het samenwerkingsverband, aanschaf van diensten of bedrijfsmiddelen en grote wijzigingen in de dienstverlening zijn aanleiding tot extra valuatie, controle en eventuele bijstelling.

Het samenwerkingsverband vraagt dit zelfde ook van de verwerkers. Hierover zijn in zowel de verwerkingsovereenkomst als het dienstverleningscontract concrete afspraken gemaakt.

3. Uitvoering

Om het informatiebeveiligings- en privacybeleid te realiseren, besteedt het samenwerkingsverband aandacht aan een aantal zaken.

3.1. Bewustzijn

Het bevorderen van bewustzijn rondom informatiebeveiliging en privacy is de verantwoordelijkheid van alle medewerkers. Het beveiligingsbewustzijn wordt vergroot door:

- Voorlichting
- Opstellen en uitdragen van gedragsregels

Het gaat daarbij om:

- Het belang van informatiebeveiliging en privacy voor het samenwerkingsverband
- Nieuwe ontwikkelingen op het gebied van informatiebeveiliging en privacy (bijvoorbeeld actuele incidenten)
- De belangrijkste veiligheidsmaatregelen rond dagelijkse werkzaamheden
- Waar mensen terecht kunnen bij incidenten of met ideeën en vragen

3.2. Incidenten en datalekken

Medewerkers die een incident of inbreuk rond informatiebeveiliging en/of privacy vermoeden, dienen dit direct te melden bij de functionaris gegevensbescherming (FG) van het samenwerkingsverband fg@swvvozaanstreek.nl, tel. nr. 075-6213725. Een vraag of suggestie over informatiebeveiliging en privacy kan ook als incident gemeld worden. Alle meldingen worden volgens een vast proces behandeld.
Na afhandeling van het incident wordt de melder ingelicht over de afhandeling daarvan.

Verzoeken rondom persoonsgegevens door externe partijen kunnen gedaan worden bij het secretariaat van het samenwerkingsverband of via email naar privacy@swvvozaanstreek.nl
Op de website van het samenwerkingsverband, staat deze loketfunctie vermeld. Externe partijen en betrokkenen kunnen bij dit loket terecht voor:

- Algemene informatie over de verwerking van persoonsgegevens.
- Verzoeken voor inzage van de eigen verwerkte persoonsgegevens en eventuele wijziging of verwijdering daarvan.

3.3. Responsible disclosure

De veiligheid van de informatiesystemen (internet en bijbehorende hardware en software) is erg belangrijk. Ondanks de zorg voor de beveiliging van deze systemen kan het voorkomen dat er toch een zwakke plek (kwetsbaarheid) is. Als een leerling of een medewerker een zwakke plek in één van deze systemen heeft gevonden, dan kan dit gemeld worden bij de privacy@swvvozaanstreek.nl, zodat zo snel mogelijk maatregelen getroffen kunnen worden.

3.4. Naleving

Schending van de wetgeving, voorschriften of regels rond informatiebeveiliging en privacy kan leiden tot corrigerende maatregelen zoals non-actiefstelling, disciplinaire straffen en beëindiging van een contract of dienstverband.

3.5. Actualiteit

Het samenwerkingsverband houdt rekening met actuele ontwikkelingen. Daarom wordt dit beleid minimaal elke twee jaar getoetst en bijgesteld door de directeur/bestuurder aan de hand van het volgende:

- De behoeften en verwachtingen van belanghebbenden in de onderwijsketen
- De status van de informatiebeveiliging als geheel (beleid, organisatie, risico's)
- De effectiviteit van de genomen maatregelen en aantoonbare werking daarvan
- Wet- en regelgeving
- Advies van de functionaris gegevensbescherming

3.6. Wet- en regelgeving

Het samenwerkingsverband voldoet aan alle wet- en regelgeving die relevant is in dit verband zoals:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs
- Code goed onderwijsbestuur VO
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht
- Alle overige wetgeving die van toepassing kan zijn

Ter uitvoering van de privacyregels heeft het samenwerkingsverband een privacyreglement vastgesteld.

3.7. De vijf vuistregels van privacy

Het samenwerkingsverband houdt zich bij het verwerken van persoonsgegevens aan de beginselen rond de verwerking persoonsgegevens (art.5 AVG). De vijf vuistregels van privacy zijn:

1. Doelbepaling en doelbinding: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt voor andere doeleinden.
2. Grondslag: verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen.
3. Dataminimalisatie: bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt. Het type persoonsgegevens staat in verhouding tot het

doel – het doel kan niet met minder of alternatieve gegevens worden bereikt. Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.

4. Transparantie: het samenwerkingsverband legt aan betrokkenen (zoals leerlingen, hun ouders en medewerkers) op transparante manier en ongevraagd verantwoording af over het gebruik van hun persoonsgegevens en het beleid daarover. Daarnaast hebben de betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens
5. Data-integriteit: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

3.8. Dataregister

Alle verwerkingen binnen en namens het samenwerkingsverband worden vastgelegd en up-to-date gehouden in een dataregister.

4. Planning & controle

Informatiebeveiliging en privacy kent een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst.

4.1 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om alle risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt het bewustzijn van de individuele medewerkers regelmatig aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Verhoging van het beveiligingsbewustzijn is tevens een (doorlopende) opdracht aan de verwerkers met het Bestuur als verwerkingsverantwoordelijke .

4.2 Classificatie en risicoanalyse

Bij het samenwerkingsverband heeft alle informatiewaarde, daarom worden alle privacygevoelige gegevens zorgvuldig behandeld en beveiligd opgeslagen. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitsaspecten die van belang zijn voor de informatievoorziening Indigo.

4.3 Incidenten en datalekken

De afhandeling van deze incidenten volgt het protocol, dat voorziet in de juiste stappen rondom de meldplicht datalekken.

4.4 Controle, naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IBP-proces. Van belang hierbij is dat leidinggevenden hun verantwoordelijkheid nemen en medewerkers aanspreken in geval van tekortkomingen. Voor de bevordering van de naleving van de AVG vervult de Functionaris Gegevensbescherming een belangrijke rol. Deze functionaris wordt aangesteld door het bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.

5 Organisatie

Het samenwerkingsverband verdeelt de rollen en verantwoordelijkheden voor informatiebeveiliging en privacy als volgt:

5.1. Medewerkers

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden.

Wij vragen medewerkers zich actief bezig te houden met informatiebeveiliging. Bijvoorbeeld door meldingen te maken van incidenten, verbetervoorstellen te doen en invloed uit te oefenen op het beleid binnen het samenwerkingsverband (zie ook hoofdstuk 3.3).

5.2. Management

De directeur-bestuurder is de eindverantwoordelijke voor informatiebeveiliging en privacy.

De directeur-bestuurder is verantwoordelijk voor:

- Het vaststellen van het informatiebeveiligingsbeleid en de daaruit volgende richtlijnen voor Het samenwerkingsverband.
- Het evalueren van de toepassing en werking van het informatiebeveiligings-beleid op basis van rapportages.

De directeur-bestuurder:

- Ziet toe op de naleving van het informatiebeveiligings- en privacybeleid door medewerkers.
- Heeft een positieve en actieve houding ten aanzien van informatiebeveiliging en privacy.
- Fungeert als voorbeeldfunctie.
- Behandelt informatiebeveiliging in bijvoorbeeld werkoverleg en beoordelingen.
- Handelt vertrouwelijke informatiebeveiligingsincidenten af.