

Bijlage 15 B Informatiebeveiligings- en privacybeleid

Samenwerkingsverband Zuid Holland West (VO 28-06)

Maart 2019

Inhoud

Voorwoord	3
1. Het belang van informatiebeveiliging en privacy	4
1.1 De reikwijdte van het informatiebeveiligings- en privacybeleid	4
1.2 Het doel van informatiebeveiliging en privacy	4
2. Het beleid.....	4
3. Kwaliteitsbewaking.....	5
4. Uitvoering.....	6
4.1. Bewustzijn	6
4.2. Naleving	6
4.3. Actualiteit	6
4.4. Wet- en regelgeving	6
4.5. Maatregelen mb.t. informatiebeveiliging privacy	6
4.6. Privacy by Design en Default	7
4.7. Verwerkers	7
4.8. Delen van gegevens met anderen	7
4.9. Incidenten en datalekken	7
4.10. Informatiebeveiliging	7
5. Organisatie	8
5.1. Medewerkers.....	8
5.2. Management	8
5.3. Planning & controle	8

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.

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 in het Samenwerkingsverband Zuid Holland West (SWVZHW). 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, vanuit een gemeenschappelijke visie en wil, de verwerking van (persoons)gegevens correct te laten verlopen. Dit betekent dat de verwerking van persoonsgegevens in overeenstemming is met dit beleid en met de geldende wet- en regelgeving (zie 4.5).

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, klant of leverancier – een inzicht in de manier waarop we omgaan met persoonsgegevens.

1.1 De reikwijdte 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 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

Om de gestelde doelen te bereiken is het beleid erop gericht op de toegang tot gegevens op een adequate manier te beveiligen en om de privacy van persoonsgegevens zo goed mogelijk te waarborgen door eenduidige opslag van gegevens en doelmatig gebruik van persoonsgegevens.

Hiertoe worden de volgende uitgangspunten gehanteerd:

- 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.
- Het samenwerkingsverband houdt zich aan alle relevante wet- en regelgeving. De directeur van het samenwerkingsverband is eindverantwoordelijk voor de bescherming van persoonsgegevens. Het samenwerkingsverband hanteert passende technische en organisatorische maatregelen voor het beschermen van diensten en in het bijzonder persoonsgegevens.

Gelet op de taakstelling van het SWVZHW is informatiebeveiliging en privacybescherming een verantwoordelijkheid van alle medewerkers.

3. Kwaliteitsbewaking

Het proces voor informatiebeveiliging is 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. Daarnaast kunnen ontwikkelingen op het gebied van wet- en regelgeving, zoals jurisprudentie, uitleg of onderzoek door de Autoriteit Persoonsgegevens of de European Data Protection Board ook reden zijn om het beleid aan te passen. Zie hiervoor ook hoofdstuk 4.4.

4. Uitvoering

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

4.1. Bewustzijn

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

- Trainen en informeren van medewerkers;
- Aansluiten bij seminars en voorlichtingsbijeenkomsten op dit gebied om expertise te vergroten.

Deze middelen dragen het volgende uit:

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

4.2. 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.

4.3. Actualiteit

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

- 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.

4.4. Wet- en regelgeving

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

- De Algemene Verordening Gegevensbescherming;
- De Uitvoeringswet Algemene Verordening Gegevensbescherming;
- Overige relevante wetgeving zoals de Wet op Passend Onderwijs.

Ter uitvoering van de privacyregels heeft het samenwerkingsverband een privacyreglement vastgesteld. Tevens is er een privacyverklaring opgesteld voor op de website van het samenwerkingsverband.

4.5. Maatregelen mb.t. informatiebeveiliging privacy

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

1. Alle gegevens voor wat betreft arrangementen en toelaatbaarheidsverklaring worden alleen opgeslagen in 1LoketVO van Onderwijs Transparant.
2. Indien het nodig is om gegevens omtrent arrangementen en toelaatbaarheidsverklaringen voor eigen gebruik tijdelijk op te slaan wordt hiervoor de H: -schijf gebruikt die alleen toegankelijk is voor de betreffende medewerker.
3. Het gebruik van e-mail met betrekking tot persoonsgegevens wordt zoveel mogelijk vermeden.
4. Het gebruik van USB-sticks wordt beperkt doordat vanaf het netwerk geen toegang tot de USB-stick mogelijk is.
5. De persoonsgegevens van medewerkers wordt in een applicatie opgeslagen en onderhouden.
6. De bewaartermijn van gegevens in 1Loket VO is drie jaar na afloop van de termijn van een arrangement of een toelaatbaarheidsverklaring.

4.6. Privacy by Design en Default

Voor het SWVZHW betekent het werken volgens privacy by design dat bij de start van het ontwerpen van een informatiesysteem of nieuwe dienst reeds rekening gehouden wordt met privacy. Systemen en diensten moeten standaard zo vormgegeven worden dat deze de hoogste mate van privacy voor de betrokkene bieden. Privacy by default is een verwant begrip, dat betrekking heeft op de standaard instellingen van een programma, website of dienst. Het SWVZHW dient er zorg voor te dragen dat deze zodanig zijn dat deze maximale privacy garanderen. In beide gevallen is het raadzaam de functionaris gegevensbescherming vooraf te raadplegen.

4.7. Verwerkers

In het geval van verwerking door externe partijen, waarbij sprake is van de verwerking van persoonsgegevens, maakt het SWVZHW afspraken over de eisen waar de verwerking aan moet voldoen. Deze afspraken voldoen aan de wet.

Wanneer gebruik gemaakt wordt van de diensten van een verwerker, legt het SWVZHW de wederzijdse verplichtingen ten aanzien van de beveiliging van de omgang met Persoonsgegevens in een schriftelijke overeenkomst met de verwerker vast (verwerkersovereenkomst). Deze overeenkomst wordt gesloten overeenkomstig de werkwijze die is vastgelegd over verwerkersovereenkomsten.

Het SWVZHW mag uitsluitend een beroep doen op verwerkers die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking aan de vereisten van deze verordening voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd.

4.8. Delen van gegevens met anderen

Het beleid van het SWVZHW is om geen persoonsgegevens te delen met andere partijen tenzij dit op basis van wetgeving en/of algemene maatregel van Bestuur wordt vereist. Hierbij kan worden gedacht aan afdracht van gegevens aan UWV, Belastingdienst, CAO gerelateerde fondsen.

4.9. Incidenten en datalekken

Medewerkers die een incident of inbreuk rond informatiebeveiliging en/of privacy vermoeden, dienen dit direct en onverwijld te melden bij de directeur. Vervolgens zal de directeur dit bespreken met de functionaris gegevensbescherming. Alle meldingen worden volgens het protocol datalekken behandeld.

Een melding van incidenten of verzoeken rondom persoonsgegevens door externe partijen kan gedaan worden bij de directeur van het SWVZHW.

4.10. Informatiebeveiliging

Het SWVZHW neemt passende organisatorische en technische maatregelen om persoonsgegevens te beveiligen tegen toevallige of onwettige vernietiging, verlies, onbevoegde openbaarmaking of toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij opzettelijk. Bij het vaststellen van de passende maatregelen speelt onder andere mee of gevoelige gegevens zoals bijzondere persoonsgegevens worden verwerkt.

Bij de beveiligingsmaatregelen wordt rekening gehouden met de stand van de techniek en de uitvoeringskosten. Daarbij houdt het SWVZHW rekening met de qua waarschijnlijkheid en ernst uiteenlopende risico's die van toepassing kunnen zijn op de verwerkte persoonsgegevens. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Iedereen binnen het SWVZHW die de beschikking krijgt over persoonsgegevens verwerkt deze slechts in opdracht van het SWVZHW en wordt geacht deze vertrouwelijk te behandelen. Voor interne en externe medewerkers geldt een geheimhoudingsplicht welke in de arbeidsovereenkomst is opgenomen.

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. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.

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

5.2. Management

De directeur is de eindverantwoordelijke voor informatiebeveiliging en privacy.

Het bestuur 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 staf:

- 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.

5.3. Planning & controle

Het samenwerkingsverband doorloopt een jaarlijkse planning- en controlecyclus voor informatiebeveiliging en privacy, deze bestaat minimaal uit de volgende activiteiten:

- Controle en rapportage
Operationele controle op de naleving van beleid en richtlijnen wordt verricht door de directie. De directeur rapporteert elk jaar aan het bestuur over de informatiebeveiliging binnen het samenwerkingsverband, de vorderingen rond implementatie en verbetering van maatregelen en de incidenten in dat kwartaal. Aan het einde van het jaar rapporteert de directeur over de algehele implementatie van informatiebeveiligingsmaatregelen.
- Interne audit
Controle op de implementatie en borging van het informatiebeveiligings- en privacybeleid en de richtlijnen en maatregelen die hieruit voortkomen. Deze vindt gedurende het jaar plaats en hierover zal nog aanvullend beleid worden opgesteld om dit inhoudelijk vorm te geven.
De uitkomst van deze audit wordt middels de risico-inventarisatie gerapporteerd aan het bestuur, de toezichthouder.