Privacy en informatiebeleid

Harderwijk, 11-1-2024

Privacy
Privacy gaat om de bescherming van persoonsgegevens conform de huidige wet- en regelgeving. Door het goed toepassen van informatiebeveiliging kan aan deze wetgeving worden voldaan. Vooral het aspect vertrouwelijkheid is hiervoor van belang. Privacy is daarom integraal onderdeel van informatiebeveiliging. Binnen VCO combineren wij beide begrippen tot één noemer: privacy- en informatiebeveiliging.

Informatiebeveiliging
Informatiebeveiliging is een proces gericht op het beschermen van VCO tegen risico's en bedreigingen met betrekking tot informatie en ict. Het richt zicht op vier aspecten:

- Beschikbaarheid; informatie en aanverwante bedrijfsmiddelen zijn toegankelijk wanneer nodig;
- Juistheid; informatie en verwerkingsmethoden bevatten zo min mogelijk fouten;
- Integriteit; gebruikers zijn eerlijk en oprecht en niet omkoopbaar. Deze personen beschikken over een intrinsieke betrouwbaarheid, hebben geen verborgen agenda en veinzen geen emoties.
- Vertrouwelijkheid; informatie is alleen toegankelijk voor diegenen die daartoe bevoegd zijn.

Doel en reikwijdte
Het Privacy- en Informatiebeveiligingsbeleid van het VCO dient twee doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van leerlingen en medewerkers waardoor beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan worden voorkomen.

Dit beleid is een leidraad voor iedereen die betrokken is bij de AVG binnen VCO. Het is van toepassing op onze eigen medewerkers, tijdelijk personeel en andere personen die een rol spelen in de stichting. Het is van toepassing op de gehele VCO-organisatie waaronder de fysieke locaties, systemen op interne en externe locaties en gegevensverzamelingen die gebruikt worden.

Het Privacy- en Informatiebeveiligingsbeleid heeft raakvlak met andere beleidsgebieden, te weten:

- Algemeen veiligheids- en beveiligingsbeleid; met als aandachtsgebieden bedrijfshulpverlening, fysieke toegang en –beveiliging, crisismanagement, huisvesting en ongevallen;
- IT-beleid; met als aandachtsgebieden de aanschaf en het beheer van ict;
- Personeels- en organisatiebeleid; met als aandachtsgebieden in- en uitstroom van medewerkers, functiescheiding en vertrouwensfuncties;
- Onderwijskundig beleid: het registreren en administreren van allerlei kindgegevens.

Dit beleid maakt tot slot duidelijk waar de verantwoordelijkheden rondom privacy- en informatiebeveiliging zijn belegd.

Uitgangspunten
VCO hanteert een aantal belangrijke uitgangspunten bij dit beleid:

- Middels dit beleid voldoen we aan alle relevante wet- en regelgeving.
- Veilig en betrouwbaar omgaan met informatie is de verantwoordelijkheid van iedereen.
- Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid.
- VCO is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt.
- VCO maakt met alle partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken over informatiebeveiliging en privacy.
- AVG – ICT is een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

- Er is een balans tussen de risico's van hetgeen we willen beschermen en de benodigde investeringen en maatregelen.
- Er is een balans tussen privacy, functionaliteit/werkbaarheid en veiligheid.

Privacy VCO

VCO hanteert de onderstaande vijf vuistregels voor privacy (ontleend aan de AVG):

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 op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. Grondslag: verwerking van Persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.
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. 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 IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun Persoonsgegevens. Daarnaast 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.

Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen. Bij alle registraties op basis van toestemming, is er door VCO aan alle 12 scholen een eenduidige procedure verstrekt.

Wet- en regelgeving

VCO voldoet met dit beleid aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs
- Wet goed onderwijs en goed bestuur PO/VO
- Wet bescherming persoonsgegevens
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

Hiernaast zijn de bepalingen van het convenant 'Digitale onderwijsmiddelen en privacy 2.0' leidend bij het maken van afspraken met leveranciers.

Privacy en informatiebeleid

Organisatie
Dit hoofdstuk beschrijft hoe de AVG binnen VCO is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

- Richtinggevend (strategisch)
- Sturend (tactisch)
- Uitvoerend (operationeel)

Voor elk niveau wordt beschreven welke wie (rollen) welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen.

Richtinggevend:
Het college van bestuur is eindverantwoordelijk voor de AVG en stelt het beleid en de maatregelen vast op het gebied van privacy en informatiebeveiliging. De toepassing en werking van het AVG-beleid wordt op basis van regelmatige rapportages door het CvB geëvalueerd.

Sturend
De Privacy Officer heeft de rol op sturend niveau. Deze geeft terugkoppeling en advies aan de CvB en stuurt de uitvoerende rollen aan. De Privacy Officer moet:

- het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling;
- de uniformiteit bewaken binnen VCO;
- het aanspreekpunt zijn voor incidenten op het gebied van privacy en informatiebeveiliging;
- de (verdere) afhandeling van incidenten binnen VCO coördineren;
- zorgdragen voor kwalitatieve aandacht voor het beleid binnen de jaarlijkse planning en controlcyclus;
- regelmatige voorlichting geven aan alle VCO-functionarissen en betrokkenen gericht op bewust handelen.

Functionaris voor Gegevensbescherming
De wettelijk verplichte functionaris voor gegevensbescherming (FG) houdt binnen VCO toezicht op de toepassing en naleving van de privacy-wetgeving. De bij wet vastgelegde taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG zorgt voor het afhandelen van vertrouwelijke informatiebeveiligingsincidenten. De FG heeft regelmatig overleg met Privacy Officer. De FG is meestal ook contactpersoon voor betrokkenen met klachten en vragen met een vertrouwelijk karakter.
Domeinverantwoordelijkheid/proceseigenaar
Binnen VCO zijn er verschillende domeinen/processen, zoals ict, personeel, administratie etcetera. Op elk van deze domeinen/processen is iemand verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

Uitvoerend
De Privacy Officer vormt een technisch aanspreekpunt voor incidenten en informatiebeveiliging.

Functioneel beheerder
De Privacy Officer is ook proceseigenaar en beheert (izsm lverancier/ServeIT) een werkpakket, bestaande uit richtlijnen, procedures en instructies.

Medewerker
Alle VCO-medewerkers tonen zich, op basis van gezond verstand, verantwoordelijk voor de informatiebeveiliging in hun dagelijkse werkzaamheden. Daarbij worden zij, waar nodig, ondersteund met checklists en formulieren. Naast verantwoordelijk gedrag, tonen medewerkers zich ook actief betrokken bij de algehele informatiebeveiliging. Dit uit zich bijvoorbeeld in het melden van incidenten / datalekken m.b.t. informatiebeveiliging, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR)

Privacy en informatiebeleid

Leidinggevende
Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het beveiligingsbeleid;
- toe te zien op de naleving van het AVG beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
- periodiek het onderwerp AVG onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
- als aanspreekpunt beschikbaar te zijn voor alle aan personeel gerelateerde AVG onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door de Privacy Officer.

Controle en rapportage
Dit privacy- en informatiebeveiligingsbeleid wordt minimaal eens per twee jaar, op aangeven van de Privacy Officer, getoetst en bijgesteld. Hierbij worden CvB, DT en staf betrokken en wordt rekening gehouden met:

- de status van de privacy- en informatiebeveiligingsbeleid als geheel (beleid, organisatie, risico's);
- de effectiviteit van de genomen maatregelen en de aantoonbare werking daarvan.

Daarnaast kent VCO een jaarlijkse planning en control cyclus voor het privacy- en informatiebeveiligingsbeleid. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het privacy- en informatiebeveiligingsbeleid wordt getoetst. De Privacy Officer is hierin coördinerend.

Voorlichting en bewustzijn
Beleid en maatregelen zijn niet voldoende om risico's op het terrein van privacy- en informatiebeveiliging uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij VCO 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, deelnemers en gasten. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de Privacy Officer, waar nodig in samenwerking met de CvB als eindverantwoordelijke.

Risicoanalyse
Bij VCO heeft alle informatie waarde, daarom treffen we de nodige beveligingsmaatregelen. Die beveliging is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn "beschikbaarheid, integriteit en vertrouwelijkheid" de kwaliteitsaspecten voor de informatievoorziening.

Incidenten en datalekken
Alle incidenten moeten worden gemeld bij de Privacy Officer. De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken. (zie VCO poster: Een datalek, wat nu?)

Controle, naleving en sancties
De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het AVG proces. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. VCO besteedt actief aandacht aan AVG bij de aanstelling, tijdens functioneringsgesprekken, met periodieke bewustwordingscampagnes, etcetera.
Voor de bevordering van de naleving van de AVG vervult de Functionaris Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door het CvB, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het CvB vast te stellen reglement.
Mocht de naleving ernstig tekort schieten, dan kan VCO de betrokken verantwoordelijke medewerker(s) een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol.

Verwerking in of buiten Europa

AVG geldt in de gehele Europese Unie, plus in Noorwegen, Liechtenstein en IJsland – samen de Europese Economische Ruimte of EER geheten. Wij werken als stichting tot nu toe niet met andere instellingen of bedrijven buiten Nederland. Gaan wij als VCO buiten de EER, dan moeten wij nagaan of deze landen veilig zijn voordat wij überhaupt met deze bedrijven in zee gaat.

Bijlage 1: Tabel rollen en taken

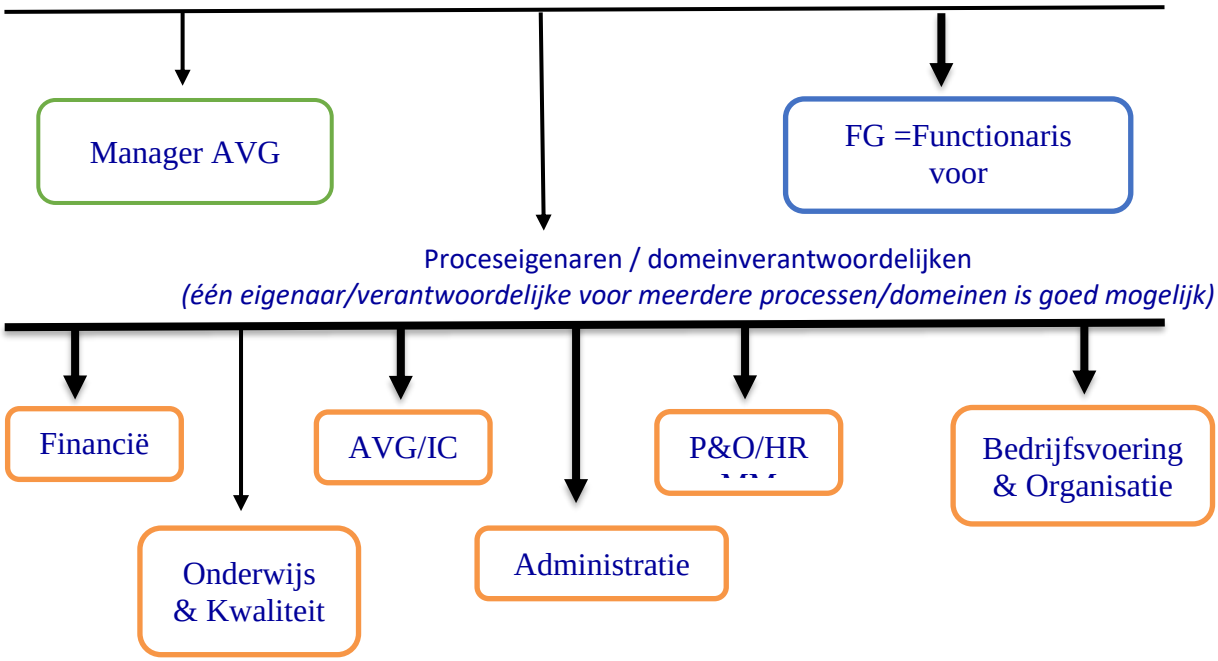
Niveau	**Wie** **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren / vastleggen**
Richtinggevend (strategisch)	College van Bestuur	• Eindverantwoordelijk • AVG-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking AVG-beleid op basis van rapportages • Organisatie AVG inrichten	• Informatiebeveiligings- en privacy beleid • Baseline / basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen
Sturend (tactisch)	AVG Manager	• Inhoudelijk verantwoordelijk voor privacy- en informatiebeveiligingsbeleid (AVG) • AVG-planning en controle • Adviseert bestuur/CvB/directie over AVG • Voorbereiden uitvoeren AVG-beleid, Risicoanalyse • Hanteren AVG normen en wijze van toetsen • Evalueren AVG-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 • Afwikkeling klachten en incidenten	Processen, richtlijnen en procedures AVG, waaronder: • activiteitenkalender • Protocol beveiligingsincidenten en datalekken • Bewerkersovereenkomsten regelen • Brief toestemming gebruik foto's en video • Opstellen informatie documentatie richting leerlingen, ouders / verzorgers • Security awareness activiteiten • Sociale media reglement • Gedragscode ICT en internetgebruik • Gedragscode medewerkers en leerlingen • Inrichten meldpunt datalekken
	FG = Functionaris voor Gegevens-bescherming	• Toezicht op naleving privacy wetgeving • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens	• Privacyreglement, • procedure AVG-incident afhandeling • Inrichten meldpunt datalekken

		• Afwikkeling klachten en incidenten	
	Domeinverant-woordelijken / Proceseigenaren	• **Risicoanalyse** *in samenwerking met AVG Manager* • 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.	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst) • Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen Vanuit de Wiki
Uitvoerend (operationeel)	AVG manager Serve-It bv.	• Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor ACG-incidenten.	
	Functioneel beheerder	• Uitvoeren taken conform gegeven richtlijnen en procedures.	
	Leidinggevende (directeur)	• Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het AVG beleid en de consequenties ervan. • Toezien op de naleving van het AVG beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Voorbeeldfunctie met positieve en actieve houding t.a.v. AVG-beleid. • Implementeren AVG-maatregelen. • periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.; • Rapporteren voortgang m.b.t. doelstellingen AVG beleid aan bestuurder	Communiceren, informeren en toezien op naleving van o.a.: • AVG in het algemeen • Regels passend onderwijs • Hoe omgaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken
	Medewerker	• Verantwoordelijk omgaan met AVG bij hun dagelijkse werkzaamheden.	

Bijlage 2: Schema AVG rollen en taken

Richtinggevend (strategisch) Bestuurder VCO & Sturend (tactisch) Manager VCO



Proceseigenaren kijken binnen hun eigen proces naar:

- Welke persoonsgegevens waar gebruikt worden
- Risicoanalyse en classificatie samen met AVG manager
- Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren
- Samen met functioneel beheerder ICT-toegangsbeleid implementeren en controleren
- T.a.v. alle punten de FG informeren

Uitvoerend (operationeel)

- **AVG manager / ServeIT bv.** : het technisch aanspreekpunt betreffende het oplossen en uitzoeken van beveiligingsincidenten (in samenwerking met AVG manager).
  LET OP: tot dusver heeft VCO dit belegd bij ServeIT → we moeten afspreken waar welke verantwoordelijkheden liggen en taken uitgevoerd worden.
- **Functioneel beheerder** (school-ict'er): uitvoeren van toegangsrechten, instellingen en procedures zoals aangegeven in goedgekeurde richtlijnen.
- **Leidinggevenden**: communiceren, informeren en toezien op naleving van de gemaakte afspraken en procedures.
- **Medewerkers**: AVG toepassen in dagelijkse werkzaamheden.

AVG is de verantwoordelijkheid van iedere VCO'er