

Informatiebeveiligings- en privacy beleid stichting ProCon (29-08-2022)

1° concept (document is nooit vastgesteld)	8-5-2018
Update (paragraaf 5 e.v.)	23-8-2022
Besproken in AVG-werkgroep	29-8-2022
2° concept (term CvB vervangen door bestuurder)	29-8-2022
Besproken in directeurenoverleg	11-10-2022
3° concept	
Voorgenomen besluit door bestuurder	
Besproken in GMR	13-02-2023
Instemming GMR	13-02-2023
Definitief besluit door bestuurder	13-02-2023
Plaatsing op (school)websites (zonder Plan van Aanpak)	09-03-2023

1	INLEIDING.....	3
1.1	TOELICHTING INFORMATIEBEVEILIGING	3
1.2	TOELICHTING PRIVACY.....	3
1.3	VERVLECHTING INFORMATIEBEVEILIGING EN PRIVACY	3
2	DOEL EN REIKWIJDTE	4
2.1	DOEL.....	4
2.2	REIKWIJDTE	4
3	UITGANGSPUNTEN	5
3.1	ALGEMENE BELEIDSUITGANGSPUNTEN.....	5
3.2	UITGANGSPUNTEN PRIVACY	6
4	WET- EN REGELGEVING.....	6
5	ORGANISATIE.....	7
6	PLAN VAN AANPAK	FOUT! BLADWIJZER NIET GEDEFINIEERD.
7	BORGEN.....	8
8	COMMUNICATIE	9
	BIJLAGE	9

1 Inleiding

Het onderwijsveld is in toenemende mate afhankelijk van informatie en (meestal geautomatiseerde) informatievoorzieningen. Ook neemt de hoeveelheid informatie toe door ontwikkelingen als gepersonaliseerd leren met ict. Deze afhankelijkheid van ict en gegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het is van belang om adequate maatregelen te nemen op het gebied van informatiebeveiliging en privacy (IBP) 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.

1.1 Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten van de informatievoorziening te garanderen.

Deze aspecten zijn:

- 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 onacceptabele risico's bij de uitvoering van onderwijs en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagooverlies.

1.2 Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens dienen beschermd te worden conform huidige wet – en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens gebruikt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die herleidbaar zijn tot een bepaald individu. Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens. 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.*

1.3 Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijk onderdeel is van privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Beide begrippen staan naast elkaar, en zijn van elkaar afhankelijk. Het onderwerp informatiebeveiliging en privacy wordt afgekort tot IBP. Dit beleid ligt ten grondslag aan de aanpak van informatiebeveiliging en privacy binnen Stichting ProCon.

2 Doel en reikwijdte

2.1 Doel

Dit beleid heeft als 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 erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij een goede balans moet zijn tussen privacy, functionaliteit en veiligheid. Uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene, met name van medewerkers en leerlingen, wordt gerespecteerd en Stichting ProCon voldoet aan relevante wet- en regelgeving.

2.2 Reikwijdte

- Het informatiebeveiligings- en het privacy beleid binnen Stichting ProCon geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing), alsmede voor alle organisatieonderdelen. Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- De nadruk van het beleid ligt op die toepassingen, die vallen onder de verantwoordelijkheid van Stichting ProCon. Het beleid heeft zowel betrekking op gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd. Daarnaast is het ook van toepassing op niet-gecontroleerde informatie waarop de school kan worden aangesproken, zoals uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites,.
- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Stichting ProCon waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op andere betrokkenen waarvan Stichting ProCon persoonsgegevens verwerkt.
- In het beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van Stichting ProCon evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het 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.
- IBP-beleid binnen Stichting ProCon heeft 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 van leerlingen, hun ouders/verzorgers en medewerkers
- Beleid inzake aanschaf en gebruik van digitale leermiddelen

3 Uitgangspunten

3.1 Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij Stichting ProCon zijn:

- Informatiebeveiliging en het privacy dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming (die 25 mei 2018 in werking treedt). De verwerking van persoonsgegevens is gebaseerd op één van de wettelijke grondslagen. Waarbij een goede balans tussen het belang van Stichting ProCon om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens van belang is.
- Binnen Stichting ProCon 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 fysieke documenten.
- De school 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 moeten goed geïnformeerd worden over de regelgeving rond het gebruik van informatie.
- Informatie heeft een waarde: financieel, economisch maar zeker ook emotioneel. De waarde van informatie wordt bij Stichting ProCon geclassificeerd. De classificatie is het uitgangspunt voor de te nemen maatregelen. Vervolgens worden mogelijke risico's geïdentificeerd door middel van een risicoanalyse, waarbij gebruik gemaakt wordt van de classificatie. Er is een balans tussen de risico's van hetgeen we willen beschermen en de benodigde investeringen en maatregelen.
- Stichting ProCon sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) bewerkersovereenkomsten af als zij persoonsgegevens ontvangen van de school. Hierbij wordt gebruik gemaakt van de meest recente versie van het convenant 'Digitale leermiddelen privacy' (www.privacyconvenant.nl) en de bijbehorende model bewerkersovereenkomst. Dit geldt ook voor overheids- en andere instellingen indien er gegevens van leerlingen of medewerkers worden verstrekt, al dan niet op wettelijke basis.
- Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht 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 imagooverlies. Stichting ProCon heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
- Informatiebeveiliging en privacy is bij Stichting ProCon een continu proces, waarbij re-

gelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

- Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt bij Stichting ProCon vanaf de start rekening gehouden met informatiebeveiliging en privacy.

3.2 Uitgangspunten privacy

De vijf vuistregels met betrekking tot de omgang van persoonsgegevens bij Stichting ProCon 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 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 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, zal Stichting ProCon aan de Betrokkene een eenduidige zogenaamde Opt-out procedure ¹ worden aangeboden.

4 Wet- en regelgeving

Stichting ProCon voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet primair onderwijs
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet

¹ Een **opt-out**regeling houdt in dat betrokkenen niets hoeven te doen om mee te doen met de regeling, maar de mogelijkheid hebben ervan af te zien.

Hiernaast zijn de bepalingen van het convenant 'Digitale onderwijsmiddelen en privacy 4.0' leidend bij het maken van afspraken met leveranciers.

5 Organisatie

ProCon heeft IBP op de volgende manier intern gestructureerd en georganiseerd:

- **Alle medewerkers**
 - Gaan zorgvuldig om met privacy, persoonsgegevens en systemen en voelen zich hiervoor verantwoordelijk.
 - Kennen de gedragsregels van ProCon en dragen deze uit bij het uitoefenen van hun functie.
- **ICT'er**
 - Is het 1^e aanspreekpunt binnen de school voor vragen over IBP.
 - Geeft voorlichting over IBP en stimuleert bewustwording.
 - Adviseert de schoolleiding of de bestuurder over IBP.
 - Werkt mee aan de evaluatie van het IBP-beleid en de maatregelen.
- **Administratief medewerker in samenwerking met IB'er**
 - Draagt zorg voor archivering/opschoning van het leerlingvolgsysteem volgens bewaartermijnenbeleid van ProCon.
- **Schooldirecteur**
 - Communiceert over het IBP-beleid met betrokkenen in de school en ziet er op toe dat dit beleid wordt uitgevoerd.
 - Ziet toe dat persoonsgegevens zorgvuldig en rechtmatig binnen de school worden verwerkt en geeft hierbij het goede voorbeeld.
 - Zorgt dat toestemmingen van betrokkenen voor gebruik beeld- en videomateriaal etc. aanwezig en actueel zijn.
 - Registreert en handelt verzoeken om inzage etc. af.
 - Informeert Security officer over incidenten/datalekken.
 - Brengt regelmatig IBP onder de aandacht in werkoverleggen, beoordelingen etc.
 - Werkt mee aan de evaluatie van het IBP-beleid en de maatregelen.
- **Security officer**
 - Is het technisch aanspreekpunt voor beveiligingsincidenten, datalekken en DPIA's (privacy risicoanalyse).
 - Werkt in overleg met de AVG-werkgroep het IBP-beleid uit in processen, richtlijnen en procedures.
 - Kent toegangsrechten toe en beheert deze.
 - Werkt mee aan de evaluatie van het IBP-beleid en de maatregelen.
- **Functionaris gegevensbescherming (FG)**
 - Informeert en adviseert bestuurder, schoolleiding, ouders en personeel over IBP.
 - Houdt toezicht dat de AVG binnen de organisatie wordt nageleefd en rapporteert daarover aan de bestuurder.
 - Brengt op verzoek advies uit over de DPIA die de bestuurder wil uitvoeren en ziet toe op de uitvoering daarvan.
 - Adviseert over de afhandeling van beveiligingsincidenten en datalekken.
 - Handelt klachten af over het gebruik van persoonsgegevens of hoe een verzoek om inzage etc. is afgewikkeld.
 - Treedt op als aanspreekpunt voor en werkt samen met AP.

In een reglement heeft ProCon de positie, taken en bevoegdheden van de FG vastgelegd, zie het Reglement Functionaris Gegevensbescherming.

- **Bestuurder**

- Stelt het IBP-beleid vast, communiceert hierover met betrokkenen in de organisatie en ziet er op toe dat dit beleid wordt uitgevoerd.
- Richt de organisatie qua IBP in en wijst rollen en taken toe.
- Ziet toe dat persoonsgegevens zorgvuldig en rechtmatig binnen de organisatie worden verwerkt en geeft hierbij het goede voorbeeld.
- Brengt regelmatig IBP onder de aandacht in werkoverleggen, beoordelingen etc.
- Evalueert regelmatig het IBP-beleid en de maatregelen.

- **Gemeenschappelijke medezeggenschapsraad (GMR)**

In de Wet medezeggenschap op scholen (WMS) wordt IBP als zodanig niet genoemd. Op grond van art. 12 lid 1 sub m WMS heeft de PGMR instemmingsrecht ten aanzien van de vaststelling of wijziging van een regeling over het verwerken van en de bescherming van persoonsgegevens van het personeel. De OGMR heeft op grond van art. 13 sub i WMS eenzelfde instemmingsrecht met betrekking tot persoonsgegevens van ouders en leerlingen. Vertaald naar de praktijk betekent dit dat de GMR instemmingsrecht heeft ten aanzien van:

1. het beleidskader IBP incl. plan van aanpak
2. privacyverklaring voor leerlingen en ouders
3. privacyverklaring voor medewerkers, studenten en vrijwilligers
4. gedragscode sociale media
5. protocol foto's en video's
6. plan van aanpak informatiebeveiliging

ProCon werkt het AVG-beleid uit in procedures, formulieren etc. Ten aanzien van deze uitwerkingen heeft de GMR informatierecht.

- **AVG-werkgroep**

ProCon heeft een AVG-werkgroep ingesteld. Deze werkgroep bestaat voorlopig uit de bestuurder en de externe deskundige van PEP Onderwijsadvies.

De AVG-werkgroep ondersteunt en begeleidt ProCon en zijn scholen bij het actualiseren en aanvullen van het huidige AVG-beleid. De AVG-werkgroep doet dit tijdelijk op basis van een plan van aanpak, zie bijlage 1.

Hierna houden de werkzaamheden van de AVG-werkgroep in beginsel op. De AVG-werkgroep zal aan het einde van schooljaar 2022-2023 inventariseren of er behoefte is om hierna het IBP-beleid of bepaalde IBP-zaken bovenschools te blijven coördineren en ondersteunen. Op basis van deze inventarisatie zal de werkgroep met een advies komen.

6 Plan van Aanpak

In bijlage 1 treft u het plan van aanpak voor het schooljaar 2022-2023 aan. In dit plan staan de verschillende stappen die ProCon gaat zetten om de doelen (zie hierboven onder 2) te bereiken. Borgen

7 Borgen

ProCon gaat werken volgens een jaarlijkse IBP PDCA-cyclus. Evaluatie en bijstelling van het IBP-beleid en de uitvoering hiervan vinden jaarlijks plaats. Eén keer per 4 jaar wordt in het kader van het nieuwe strategische beleidsplan ook het beleidskader IBP (dit document) geëvalueerd en indien nodig geactualiseerd.

8 Communicatie

ProCon vindt het belangrijk om alle betrokkenen goed te informeren over IBP. In het plan van aanpak vindt u informatie over de wijze waarop ProCon en zijn scholen met leerlingen, ouders, medewerkers, studenten, vrijwilligers en (G)MR willen communiceren, zie bijlage ..

Bijlage 1. Plan van Aanpak implementatie