

CLASSIFICATIE VAN PERSOONSgegevens

basisschool Sancta Maria

Deze nota maakt deel uit van het informatieveiligheid- en privacybeleid (IVPB).

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	2018-05-26	GELDIG		

1 Inleiding

1.1 Situering

Door een classificatie van persoonsgegevens te maken, kan men op onze school op een gestructureerde manier de beveiliging van deze gegevens vorm geven. De classificatie gebeurt op basis van drie aspecten:

- beschikbaarheid;
- integriteit;
- vertrouwelijkheid.

Men spreekt ook wel eens van een BIV-classificatie. Voor elk aspect wordt in dit beleid een classificatie in niveau's gehanteerd, bv. **laag – midden – hoog**.



Op basis van de in deze nota uitgewerkte classificatie, bepaalt men op onze school de nodige organisatorische en technische maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid gepast te waarborgen.

Deze nota valt onder de eindverantwoordelijkheid van KBMS Leuven vzw.

1.2 Hoe wordt het classificatieniveau bepaald?

Dit doen we op onze school door gebruik te maken van de vragen, zoals deze zijn opgesteld voor het respectievelijke schema (zie onderstaande). Het is hierbij in zekere zin belangrijker om met een aantal mensen te praten over deze vragen, dan een exacte inschatting te maken. Door erover te praten kweek je bewustwording en ga je anders naar de processen kijken.

1.3 Welke persoonsgegevens worden er verwerkt?

Samengevat verwerkt onze school de onderstaande categorieën van persoonsgegevens: (de volledige lijst kan ingekeken worden bij Jan Leenaerts)

1.3.1 Leerlingen

1.3.2 Ouder(s) / voogd

1.3.3 Personeel

1.3.4 Oud-leerlingen

1.3.5 Oud-personeel

1.3.6 PWA-ers

1.3.7 Vrijwilligers

1.3.8 Contractuelen

1.3.9 Sollicitanten

1.3.10 Stagiairs

2 Beschikbaarheid

2.1 Omschrijving

Hiermee bedoelen we de mate waarin de gegevens en diensten beschikbaar zijn, zodanig dat het onderwijsgebeuren ongestoord voort kan gaan.

Deelaspecten hiervan zijn:

- **Continuïteit:** de mate waarin de beschikbaarheid gewaarborgd is;
- **Portabiliteit:** de mate waarin de overdraagbaarheid van informatie naar andere gelijksoortige technische infrastructuren gewaarborgd is;
- **Herstelbaarheid:** de mate waarin de informatie of dienst tijdig en volledig hersteld kan worden in geval van onderbrekingen, pannes, onderhoud, ...

Voor de beschikbaarheid komt de classificatie respectievelijk overeen met: **niet nodig, onbelangrijk, belangrijk, essentieel.**

Niveau 1: Beschikbaarheid is niet nodig	Niveau 2: Beschikbaarheid is onbelangrijk	Niveau 3: Beschikbaarheid is belangrijk	Niveau 4: Beschikbaarheid is noodzakelijk
<i>Het systeem of de informatie is niet (meer) nodig voor de werking van de instelling.</i>	<i>Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende meerdere dagen brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers of haar leerlingen.</i>	<i>Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een dag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar leerlingen.</i>	<i>Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een werkdag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar leerlingen.</i>
Tussen 0 en 2	Tussen 3 en 7	Tussen 8 en 12	Tussen 13 en 15

Het volledige overzicht kan ingegeken worden bij Jan Leenaerts.

2.2 Beschikbaarheidsschema

Dit schema moet per toepassing ingevuld worden.

Plaats een 'x' in de bijhorende kolom om de classificatie te maken, en motiveer elke vraag. Tel het eindtotaal op om de classificatie van de toepassing te bekomen (zie tabel in § 2.1). *0 staat voor "niet van toepassing".*

Toepassing 1: Leerlingvolgsysteem (schoolonline)

Toepassing 2: Boekhouding (Count-e)

Toepassing 3: Ministerie van onderwijs (WISA)

Toepassing 4: Schoolwebsite (one.com)

Toepassing 5: Klasblogs (blogspot, wordpress)

Toepassing 6: Zorgdossiers (CLB)

Toepassing 7: Online werken in de klas (Bingel => Van In)

Toepassing 8: Oude papieren dossiers van lln. en lkr. (school)

De volledige oplijsting per toepassing kan ingekeken worden bij Jan Leenaerts.

3 Integriteit

3.1 Omschrijving

Hiermee wordt bedoeld of de gegevens correct en actueel zijn. Deelaspecten hiervan zijn:

- **Juistheid:** de mate waarin overeenstemming van de presentatie van gegevens/informatie in IT-systemen ten opzichte van de werkelijkheid is gewaarborgd;
- **Volledigheid:** de mate van zekerheid dat de volledigheid van gegevens/informatie in het object gewaarborgd is;
- **Waarborging:** de mate waarin de correcte werking van de IT-processen is gewaarborgd.

Voor de integriteit komt de classificatie respectievelijk overeen met: **niet noodzakelijk, noodzakelijk, vereist, absoluut.**

Niveau 1: Integriteit is niet noodzakelijk.	Niveau 2: Integriteit is noodzakelijk.	Niveau 3: Integriteit is vereist.	Niveau 4: Integriteit is absoluut.
<i>Blijvende juistheid van informatie (vanaf de bron tot het laatste gebruik) is gewenst, maar hoeft niet gegarandeerd te zijn. Indien informatie niet correct is, leidt dit tot beperkte schade.</i>	<i>Blijvende juistheid van informatie moet maximaal gewaarborgd zijn. Sommige toleranties zijn toelaatbaar. Juistheid van informatie is belangrijk, maar niet kritisch. Het is niet noodzakelijk dat correctheid onbetwistbaar aangetoond kan worden. Indien informatie niet correct is, kan de organisatie substantiële schade lijden.</i>	<i>Informatie moet gegarandeerd correct zijn. Het is echter niet noodzakelijk dat correctheid onbetwistbaar aangetoond kan worden. Indien informatie niet correct is, kan de organisatie ernstige schade lijden.</i>	<i>Informatie moet gegarandeerd correct zijn. Informatie waarbij het noodzakelijk is dat de correctheid niet betwist kan worden, zoals de uitslagen van toetsen, examens, onomkeerbare financiële transacties. Indien informatie niet correct is, kan de organisatie ernstige schade lijden.</i>
Tussen 0 en 2	Tussen 3 en 7	Tussen 8 en 13	Tussen 14 en 18

3.2 Integriteitsschema

Dit schema moet per toepassing ingevuld worden.

Plaats een 'x' in de bijhorende kolom om de classificatie te maken, en motiveer elke vraag. Tel het eindtotaal op om de classificatie van de toepassing te bekomen (zie tabel in § 3.1). 0 staat voor "niet van toepassing".

Toepassing 1: leerlingvolgsysteem (schoolonline)

Toepassing 2: Boekhouding (Count-e)

Toepassing 3: Ministerie van onderwijs (WISA)

Toepassing 4: Schoolwebsite (one.com)

Toepassing 5: Klasblogs (blogspot, wordpress)

Toepassing 6: Zorgdossiers (CLB)

Toepassing 7: Online werken in de klas (Bingel => Van In)

Toepassing 8: oude papieren dossiers van lln. en lkr. (school)

De volledige oplistings per toepassing kan ingekeken worden bij Jan Leenaerts.

4 Vertrouwelijkheid

4.1 Omschrijving

Hiermee wordt de mate bedoeld, dat de juiste personen en systemen toegang krijgen tot de gegevens in kwestie.

Deelaspecten hiervan zijn:

- **Authenticatie:** is het proces waarbij je je identiteit gaat bewijzen (ben je wel diegene die je beweert te zijn). Vaak doen we dit door combinatie van een gebruikersnaam en een wachtwoord.
- **Autorisatie:** is een proces waarbij onderzocht wordt of je voldoende rechten hebt of toestemming hebt voor hetgeen je wilt doen. Bijvoorbeeld: een leerkracht zal toestemming hebben om in het puntenboek van de klas te schrijven, de leerling mag alleen zijn eigen punten lezen. Enkel de zorgverantwoordelijke en de directie kan in het zorgdossier van een leerling schrijven.
- **Auditing (Controleerbaarheid):** is het proces waarmee je kan nagaan wie wat waar, wanneer en waarmee doet. Vaak heb je hiervoor een hulpmiddel nodig dat je kan vertellen wat er op elk moment gebeurde. Dit kan onder meer in de vorm van een logboek.

Voor de vertrouwelijkheid komt de classificatie respectievelijk overeen met: **openbaar, intern, vertrouwelijk, geheim.**

Niveau 1: Informatie is openbaar	Niveau 2: Informatie is intern	Niveau 3: Informatie is vertrouwelijk.	Niveau 4: Informatie is geheim.
<i>Openbaar worden van gegevens leidt tot weinig of geen schade voor een instelling of betrokkene.</i>	<i>De organisatie, instelling of betrokkene kan niet meteen substantiële schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen, maar informatie mag wel alleen toegankelijk zijn voor personen die hier vanuit hun functie toegang toe moeten hebben (need-to-know basis).</i>	<i>De organisatie, instelling of betrokkene kan substantiële schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag alleen toegankelijk zijn voor personen die hier vanuit hun functie toegang toe moeten hebben (need-to-know basis).</i>	<i>De organisatie, instelling of betrokkene kan ernstige schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag uitsluitend toegankelijk zijn voor een zeer geselecteerde groep personen. Hieronder vallen onder andere bijzondere persoonsgegevens.</i>

4.2 Vertrouwelijkheidschema

Hieronder staat de classificatie van categorieën van persoonsgegevens, zoals ze op onze school gehanteerd wordt.

De volledige lijst kan ingekeken worden bij Jan Leenaerts.

5. Inventaris van alle toepassingen en verwerkers waarvoor er persoonsgegevens verwerkt worden, en hun bewaartermijnen

toepassingen	verwerkers	bewaartermijn
Leerlingvolgsysteem	Schoolonline	Voor altijd
Boekhouding	Count-e	"
Ministerie van onderwijs	Wisa (webedison voor leerkrachten, discimus voor leerlingen, schoolware)	"
Schoolwebsite	One.com	"
Klasblogs	Blogspot Wordpress	"
Online werken in de klas	Bingel	1 jaar
Oude papieren dossiers van leerlingen en leerkrachten	School zelf	Voor altijd