

1. Beleid

De normen in het domein Beleid geven je sturing en richting om privacy binnen je school in te richten in lijn met de beginselen van de Algemene Verordening Gegevensbescherming (AVG). Ze vormen de randvoorwaarden voor de invulling van de normen uit de andere domeinen. En ze zorgen ervoor dat jouw organisatie de processen en bijbehorende verantwoordelijkheden en risico's in kaart brengt en vastlegt in beleidsstukken. Deze informatie moet voor alle medewerkers goed vindbaar en begrijpelijk zijn.

Wie is verantwoordelijk:

Eindverantwoordelijk: Schoolbestuur

Verantwoordelijk voor uitvoering: Privacy Officer of IBP-adviseur

Geraadpleegd: (G)MR, FG

Geïnformeerd: Proceseigenaren, alle medewerkers, Raad van Toezicht

BL.01 Privacybeleid

Norm

Er is een privacybeleid vastgesteld voor de gehele organisatie.

Waarom is dit nodig?

In het onderwijs worden veel persoonsgegevens verwerkt. Met een privacybeleid geef je invulling aan de verplichtingen die voortvloeien uit de AVG en andere (onderwijs)wetgeving. Het privacybeleid is het interne kompas voor hoe je als organisatie met persoonsgegevens omgaat. Je zorgt er daarmee voor dat je gegevens van medewerkers en leerlingen op een rechtmatige en zorgvuldige manier verwerkt.

1 - Ad hoc

1 – Ad hoc

a) Het privacybeleid bestaat in concept, of er is geen beleid opgesteld.

2 - Herhaalbaar

2 – Herhaalbaar

a) Privacybeleid is uitgewerkt, maar nog onvolledig, verouderd, (nog) niet formeel vastgesteld en/of alleen bekend bij enkele individuen in de organisatie.

3 - Bepaald (streefniveau)

3 – Bepaald

- a) Het privacybeleid is actueel en beschrijft hoe de organisatie uitvoering geeft aan de privacybeginselen die in art 5 lid 1 AVG zijn vastgelegd.
- b) Het privacybeleid beschrijft de verplichtingen zoals doelbinding, rechtmatigheid, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en vertrouwelijkheid die op de organisatie rusten op grond van relevante privacywetgeving en beschrijft hoe de organisatie uitvoering geeft aan deze verplichtingen.
- c) Het privacybeleid is formeel door het schoolbestuur vastgesteld en organisatiebreed bekend, makkelijk vindbaar en makkelijk te begrijpen.
- d) In het beleid is rekening gehouden met (sector)specifieke wet- en regelgeving, indien van toepassing.
- e) Wijzigingen in het beleid worden gecommuniceerd.

4 - Beheerst

4 – Beheerst

a) Het privacybeleid wordt periodiek, maar ten minste eenmaal per 36 maanden, geëvalueerd en zo nodig herzien. Een evaluatierapport wordt opgesteld voor het schoolbestuur.

b) De actualiteit en kwaliteit van het privacybeleid worden getoetst in samenhang met overige beleidsstukken en vice versa. Veranderde wet- en regelgeving en doelstellingen van de organisatie vormen hier een onderdeel van.

5 - Continu verbeteren

5 – Continu verbeteren

a) Er wordt in het privacybeleid rekening gehouden met toekomstige veranderende wet- en regelgeving, doelstellingen en visie van de organisatie.

b) Er wordt actief verbinding gezocht met andere (vergelijkbare) organisaties om kennis, ervaring en best practices uit te wisselen.

Aan de slag

1. Stel een privacybeleid op dat voldoet aan de eisen zoals verwoord in de Toelichting op het template IBP-beleid. Je kunt hiervoor gebruikmaken van het template IBP-beleid.
2. Laat het schoolbestuur het beleid vaststellen.
3. Controleer ten minste eens per twee jaar of er wijzigingen nodig zijn in het privacybeleid. Leg de controle vast in het document inclusief eventuele wijzigingen die zijn doorgevoerd.
4. Bespreek ten minste een keer per jaar op elke individuele school die onder het schoolbestuur valt in een teamoverleg het privacybeleid. Stel zo vast of het beleid toereikend is en of het gevolgd wordt binnen de organisatie.
5. Plaats het beleid goed vindbaar op intranet.
6. Informeer elke medewerker tijdens het inwerkproces over het privacybeleid.
7. Neem waar nodig en relevant het privacybeleid bij uitbesteding van dienstverlening mee in de eisen.

Referentie naar andere normen en kaders

AVG Art. 24 lid 2

Link naar relevante IB normen

GO.02

BL.02 Rollen, taken en verantwoordelijkheden

Norm

Rollen, taken en verantwoordelijkheden met betrekking tot privacy binnen de organisatie zijn benoemd, belegd en vastgelegd in het privacybeleid.

Waarom is dit nodig?

Om de doelen van je privacybeleid te bereiken is het belangrijk dat je duidelijke rollen, taken en verantwoordelijkheden voor privacy benoemt, toewijst en vastlegt binnen je school. Op die manier weet iedereen wat er van hen wordt verwacht met betrekking tot privacy. Dit helpt bij het creëren van een digitaal veilige schoolomgeving voor leerlingen en medewerkers, en draagt eraan bij dat je school voldoet aan de AVG.

1 - Ad hoc

1 – Ad hoc

a) Rollen, taken en verantwoordelijkheden met betrekking tot privacy zijn niet duidelijk gedefinieerd en toegewezen binnen de organisatie of zijn niet gedocumenteerd.

2 - Herhaalbaar

2 – Herhaalbaar

a) Rollen, taken en verantwoordelijkheden zijn binnen de organisatie deels of informeel belegd en/of zijn sterk afhankelijk van de ondersteunende (centrale) privacyorganisatie of Privacy Officers.

3 - Bepaald (streefniveau)

3 – Bepaald

a) Rollen, taken en verantwoordelijkheden met betrekking tot privacy zijn formeel benoemd, belegd en vastgelegd in het privacybeleid en organisatiebreed bekend.

b) Vastgelegd is dat het schoolbestuur eindverantwoordelijk is voor privacy binnen de organisatie en dat managers verantwoordelijk zijn voor privacy binnen hun managementdomein.

c) Binnen de organisatie is vastgesteld welke functionaris bevoegd is om keuzes te maken op het gebied van privacyrisico's (waaronder het (laten)uitvoeren van (pre-)DPIA's), het treffen van mitigerende maatregelen en het accepteren van restrisico's.

4 - Beheerst

4 – Beheerst

a) Het management legt aantoonbaar verantwoording af over zijn taken en verantwoordelijkheden met betrekking tot privacy.

b) De organisatie evalueert periodiek of de rollen, taken en verantwoordelijkheden met betrekking tot privacy nog passend en effectief zijn, en voert indien nodig verbeteringen door.

5 - Continu verbeteren

5 – Continu verbeteren

a) De organisatie monitort proactief of rollen, taken en verantwoordelijkheden met betrekking tot privacy nog passend en actueel zijn, in lijn met ontwikkelingen én met wet- en regelgeving.

b) Rollen, taken en verantwoordelijkheden met betrekking tot privacy zijn expliciet opgenomen in de functieprofielen van de organisatie, waarmee ze een integraal onderdeel zijn van de taken en verantwoordelijkheden van elke medewerker.

c) De organisatie hanteert een lessons learned benadering om haar privacyverantwoordelijkheden continu te verbeteren, op basis van ervaringen uit het verleden en verwachtingen voor de toekomst.

Aan de slag

1. Leg de rollen, taken en verantwoordelijkheden met betrekking tot privacy vast in het IBP-beleid.
2. Leg in de beschrijving van rollen, taken en verantwoordelijkheden met betrekking tot privacy vast dat het schoolbestuur eindverantwoordelijk is voor privacy binnen de organisatie en dat directeuren/rectoren verantwoordelijk zijn voor privacy op hun eigen school.
3. Leg in de beschrijving van rollen, taken en verantwoordelijkheden met betrekking tot privacy vast welke functionaris van het schoolbestuur het mandaat heeft gekregen om keuzes te maken op het gebied van privacyrisico's en het treffen van mitigerende maatregelen en accepteren van restrisico's.

Referentie naar andere normen en kaders

AVG Art. 24 lid 1

Link naar relevante IB normen

OR.01

BL.03 Risico's verwerking persoonsgegevens

Norm

De organisatie heeft inzicht in de risico's van de verwerking van persoonsgegevens en behandelt deze op een adequate wijze.

Waarom is dit nodig?

Het verwerken van persoonsgegevens brengt onvermijdelijk risico's met zich mee voor de privacy van betrokkenen. Een (jaarlijkse) risico-inventarisatie geeft je inzicht in de kans op en impact van deze risico's. Op basis van de geconstateerde risico's kun je passende organisatorische en technische maatregelen treffen om de risico's te minimaliseren. Hierdoor kun je waarborgen en aantonen dat je voldoet aan de AVG.

1 - Ad hoc

1 – Ad hoc

- a) Er is geen gedocumenteerd proces binnen de organisatie voor het identificeren, beoordelen en beheren van risico's in de verwerking van persoonsgegevens.
- b) De organisatie heeft beperkt inzicht in de risico's bij de verwerking van persoonsgegevens.

2 - Herhaalbaar

2 – Herhaalbaar

- a) De organisatie heeft een informeel proces geïmplementeerd voor het identificeren, beoordelen en beheren van hoge risico's in de verwerking van persoonsgegevens.

3 - Bepaald (streefniveau)

3 – Bepaald

- a) Het schoolbestuur heeft een formeel proces beschreven voor het identificeren, beoordelen en beheren van risico's in de verwerking van persoonsgegevens. Dit proces is niet exclusief voor hoge risico's.
- b) In het proces is opgenomen dat vastgelegd wordt welke functionaris operationeel verantwoordelijk is voor opvolging van benodigde maatregelen.
- c) De organisatie beschikt over een beoordelingskader om risico's te mitigeren.
- d) Er is een volledige registratie van hoge risico's.
- e) Risicoacceptatie geschiedt op het juiste managementniveau.

4 - Beheerst

4 – Beheerst

- a) Er is een volledige registratie van alle risico's, ook de lage geïdentificeerde risico's.
- b) Alle geïdentificeerde risico's worden volledig geregistreerd en systematisch beheerd.
- c) De doeltreffendheid van het proces voor het identificeren, beoordelen en beheren van risico's én de risicobeheersmaatregelen worden periodiek beoordeeld en zo nodig aangepast.

5 - Continu verbeteren

5 – Continu verbeteren

- a) De organisatie heeft een proactieve en geïntegreerde benadering van risicobeheer, waarbij de risico's in de verwerking van persoonsgegevens continu worden gemonitord en aangepast in reactie op veranderingen in zowel de interne organisatie als het externe landschap.

b) Het management controleert en evalueert continu de doeltreffendheid van zijn risicobeheersysteem en voert waar nodig verbeteringen door.

Aan de slag

1. Stel een procedure op voor het identificeren, beoordelen en beheren van lage, middelgrote en hoge risico's bij de verwerking van persoonsgegevens. Neem hierin een beoordelingskader op om risico's te mitigeren.
2. Leg in de procedure vast welke functionaris operationeel verantwoordelijk is voor elk proces waarin persoonsgegevens worden verwerkt. Deze functionaris is ook verantwoordelijk voor de opvolging van de benodigde maatregelen en acceptatie van (rest)risico's.
3. Zorg voor vastlegging van de uitkomsten van de risicoanalyse.

Referentie naar andere normen en kaders

AVG Art.24 lid 1

Link naar relevante IB normen

RM.01, RM.02, RM.03

2. Processen

Het schoolbestuur moet een actueel beeld hebben van welke persoonsgegevens er in welke processen worden verwerkt. Daarmee heb je controle over het gebruik van die persoonsgegevens en inzicht in de risico's die daarmee samenhangen. Op basis van deze informatie kun je passende maatregelen nemen om de risico's te beperken. De beschrijving van de processen zijn actueel, de werkinstructies worden gedeeld en nageleefd, en processen met een hoog risico worden tijdig getoetst.

Wie is verantwoordelijk:

Eindverantwoordelijk: Schoolbestuur

Verantwoordelijk voor de uitvoering: Privacy Officer of IBP-adviseur, proceseigenaar

Geraadpleegd: FG, verwerker, informatiemanager

Geïnformeerd: Proceseigenaren, relevante medewerkers

PR.01 Operationele processen

Norm

De organisatie heeft de operationele processen waarin persoonsgegevens worden verwerkt in beeld en beschreven.

Waarom is dit nodig?

Als je de operationele primaire en secundaire processen beschrijft waarin persoonsgegevens worden verwerkt, bevordert dat de kwaliteit en veiligheid ervan. Je houdt daarmee grip op de processen en kunt controleren of gegevens volgens de AVG worden verwerkt. Afhankelijk van de aard, omvang, context en het doel van een proces kan de beschrijving op hoofdlijnen of meer gedetailleerd zijn.

1 - Ad hoc

1 – Ad hoc

a) De organisatie heeft geen systematische en gestructureerde aanpak voor het identificeren en documenteren van operationele processen waarin persoonsgegevens worden verwerkt.

b) Er is beperkt of geen inzicht in de processen waarin persoonsgegevens worden verwerkt, met name in de processen met een hoog risico voor de betrokkenen.

2 - Herhaalbaar

2 – Herhaalbaar

a) De organisatie heeft een gedeeltelijk systematische en gestructureerde aanpak voor het identificeren en documenteren van operationele processen waarin persoonsgegevens worden verwerkt. Deze aanpak wordt niet consistent en/of organisatiebreed gehanteerd.

b) Voor enkele processen waarin persoonsgegevens worden verwerkt is een procesbeschrijving met daarin minimaal een titel van het proces en een verantwoordelijke proceseigenaar, maar er is geen centraal overzicht of register van deze processen.

3 - Bepaald (streefniveau)

3 – Bepaald

a) De organisatie hanteert organisatiebreed een systematische en gestructureerde aanpak voor het identificeren en documenteren van processen waarin persoonsgegevens worden verwerkt en heeft inzicht in alle processen waarin persoonsgegevens worden verwerkt. Ten minste de processen met een hoog risico voor betrokkenen zijn beschreven en vastgelegd.

b) Proceseigenaren zijn aangewezen en zijn verantwoordelijk voor de periodieke evaluatie van de procesbeschrijving en passen deze zo nodig aan.

4 - Beheerst

4 – Beheerst

a) De organisatie heeft alle operationele processen waarin persoonsgegevens worden verwerkt vastgelegd en beschreven (niet alleen die met hoog risico).

b) De organisatie voert periodieke evaluaties uit van alle processen waarin persoonsgegevens worden verwerkt, om de bescherming van persoonsgegevens te waarborgen, en voert waar nodig verbeteringen door.

c) Binnen een vastgesteld interval wordt geëvalueerd of de beschrijving van het proces aansluit bij de praktijk.

d) Proceseigenaren informeren proactief over de realisatie van uitgevoerde wijzigingen naar aanleiding van evaluaties.

5 - Continu verbeteren

5 – Continu verbeteren

a) Het management ziet het belang in van procesmatig werken en het actueel houden van operationele processen en stuurt hier actief op.

b) Het management (eventueel in samenspraak met proceseigenaren) houdt toekomstige ontwikkelingen in beeld en laat deze proactief meenemen in de (her)definitie van processen en aanwijzing van proceseigenaren.

c) Er wordt proactief geborgd dat wijzigingen en initiatieven die niet voldoen aan het privacybeleid worden geïdentificeerd en opgelost.

Aan de slag

1. Hanteer organisatiebreed een systematische en gestructureerde aanpak voor het identificeren en documenteren van processen waarin persoonsgegevens worden verwerkt.

2. Toets alle processen waarin persoonsgegevens worden verwerkt aan de privacybeginselen van art. 5 lid 1 AVG.

3. Laat iedereen die verantwoordelijk is voor een proces waarin persoonsgegevens worden verwerkt dit minimaal éénmaal per jaar evalueren, en zo nodig de procesbeschrijving aanpassen.

Referentie naar andere normen en kaders

AVG Art.24 lid 1

Link naar relevante IB normen

PR.02 Verwerkingsregister opzet en vastlegging verwerkingen

Norm

De organisatie houdt een verwerkingsregister bij dat voldoet aan de wettelijke eisen.

Waarom is dit nodig?

Een volledig verwerkingsregister geeft je inzicht in de verwerking van alle persoonsgegevens binnen de school. Met dit inzicht kun je per verwerkingsactiviteit de juiste maatregelen treffen. Dit vermindert de risico's op ongeautoriseerde toegang, openbaarmaking van gevoelige informatie en onrechtmatige verwerking. Daarmee kan het schoolbestuur aantonen dat het voldoet aan dit deel van de privacywetgeving.

1 - Ad hoc

1 – Ad hoc

- a) Er is geen verwerkingsregister of er zijn geen verwerkingen bijgehouden.
- b) Wettelijk vereiste onderdelen, rollen voor verwerking (verwerkingsverantwoordelijke, verwerker, gezamenlijke verwerkingsverantwoordelijken) en verwijzingen naar operationele processen zijn niet duidelijk of ontbreken.

2 - Herhaalbaar

2 – Herhaalbaar

- a) Er is een (gedeeltelijk) ingevuld verwerkingsregister, maar niet alle wettelijk vereiste onderdelen zijn aanwezig.
- b) Voor (sommige) verwerkingen zijn de rollen voor verwerking niet duidelijk of niet gedocumenteerd.
- c) Niet alle verwerkingen zijn getoetst aan de privacybeginselen van art. 5 lid 1 AVG.

3 - Bepaald (streefniveau)

3 – Bepaald

- a) Het verwerkingsregister bevat minimaal alle wettelijk vereiste onderdelen (art. 30 lid 1 AVG voor de verwerkingsverantwoordelijke of voor de verwerker lid 2 AVG).
- b) Voor elke vastgelegde verwerking is duidelijk wie de verwerkingsverantwoordelijke, de verwerker of de gezamenlijke verwerkingsverantwoordelijken zijn.
- c) Tenminste alle verwerkingen met hoge risico's zijn vastgelegd en getoetst aan de privacy beginselen van art. 5 lid 1 AVG.

4 - Beheerst

4 – Beheerst

- a) Alle verwerkingen zijn vastgelegd.
- b) Indien de Autoriteit Persoonsgegevens (AP) inzicht in het verwerkingsregister vraagt, kan dit op eenvoudige wijze worden voorgelegd.

5 - Continu verbeteren

5 – Continu verbeteren

- a) Het verwerkingsregister wordt actief gebruikt voor risicobeheer en besluitvorming. Het is niet alleen een database voor naleving, maar een belangrijk instrument voor de privacy cultuur binnen de organisatie.
- b) In het verwerkingsregister staan verwijzingen naar uitgevoerde (pre-)DPIA's, verwerkersovereenkomsten en

andere relevante overeenkomsten.

c) Het register bevat volledige en actuele verwijzingen naar alle operationele processen waarbinnen persoonsgegevens worden verwerkt.

Aan de slag

1. Houd een verwerkingsregister bij en neem daarin alle processen op waarin persoonsgegevens worden verwerkt. Zorg ervoor dat het register voldoet aan alle wettelijk vereiste onderdelen (art. 30 lid 1 en 2 AVG).
2. Leg in het register de naam of namen vast van de (gezamenlijk) verwerkingsverantwoordelijke of verwerker (leverancier) van elke verwerking.
3. Toets verwerkingen met een hoog risico aan de privacybeginselen van art. 5 lid 1 AVG.

Referentie naar andere normen en kaders

AVG Art.30

Link naar relevante IB normen

PR.03 Verwerkingsregister actualisatie

Norm

De organisatie houdt het verwerkingsregister continu actueel.

Waarom is dit nodig?

Met een nauwkeurig bijgewerkt en actueel verwerkingsregister heeft je school altijd een correct overzicht van de omvang en aard van de verwerking van persoonsgegevens. Met dit inzicht kun je per verwerkingsactiviteit de juiste maatregelen treffen. Zo verklein je het risico dat persoonsgegevens in verkeerde handen komen of onrechtmatig worden verwerkt. Wanneer zich toch incidenten voordoen, kun je met het actuele verwerkingsregister snel en adequaat optreden.

1 - Ad hoc

1 – Ad hoc

a) Er is geen duidelijke procedure voor het bijhouden van nieuwe en gewijzigde verwerkingen in het verwerkingsregister.

2 - Herhaalbaar

2 – Herhaalbaar

a) Er is een informele procedure voor het bijhouden van nieuwe en gewijzigde verwerkingen in het verwerkingsregister, maar deze wordt niet consequent toegepast.

b) Het verwerkingsregister is niet up-to-date omdat wijzigingen in verwerkingen niet altijd tijdig in het verwerkingsregister worden opgenomen.

c) De verantwoordelijkheden voor het bijhouden van het verwerkingsregister zijn toegewezen, maar worden niet actief opgepakt.

3 - Bepaald (streefniveau)

3 – Bepaald

a) Er is een vastgestelde procedure die definieert hoe en wanneer nieuwe en gewijzigde verwerkingen in het verwerkingsregister worden opgenomen.

b) Bij wijzigingen in een opgenomen verwerkingsactiviteit wordt opnieuw getoetst of de verwerking in overeenstemming is met de privacybeginselen van art. 5 lid 1 AVG.

- c) Er is vastgesteld met welke frequentie het verwerkingsregister wordt beoordeeld op volledigheid en actualiteit, en welke functionaris verantwoordelijk is voor deze beoordeling.
- d) Wijzigingen en nieuwe initiatieven waarbij persoonsgegevens worden verwerkt, worden direct in het register opgenomen.

4 - Beheerst

4 – Beheerst

- a) Het actueel houden van het verwerkingsregister is, waar van toepassing, volledig geïntegreerd in alle processen van de organisatie. Wijzigingen en nieuwe initiatieven waarbij persoonsgegevens worden verwerkt, worden direct in het register opgenomen.

5 - Continu verbeteren

5 – Continu verbeteren

- a) De organisatie heeft een tool ingezet voor het bijhouden en auditen van het verwerkingsregister.

Aan de slag

1. Stel een procedure vast om het verwerkingsregister actueel te houden. Leg hierin in vast hoe en wanneer nieuwe en gewijzigde verwerkingen worden opgenomen.
2. Stel in de procedure vast wie verantwoordelijk is om wijzigingen in gegevensverwerkingen te (laten) wijzigen in het register.
3. Toets bij wijzigingen in het register of de verwerking in overeenstemming is met de privacybeginselen van art. 5 lid 1 AVG.

Referentie naar andere normen en kaders

AVG Art.30

Link naar relevante IB normen

PR.04 Identificatie risico's gegevensverwerking met behulp van pre-DPIA's

Norm

De organisatie identificeert systematisch of verwerkingen een hoog risico in kunnen houden voor de rechten en vrijheden van betrokkenen.

Waarom is dit nodig?

Het systematisch beoordelen en identificeren van risico's bij nieuwe of gewijzigde gegevensverwerkingen bevordert de privacybescherming van betrokkenen. Een pre-DPIA helpt je om in te schatten of een verwerking een hoog risico kan opleveren voor de privacy van betrokkenen en dit eenvoudig en gemotiveerd vast te leggen. Wanneer blijkt dat er waarschijnlijk sprake is van een hoog risico, voer je een volledige DPIA uit.

1 - Ad hoc

1 – Ad hoc

- a) Er is geen procedure of methode (zoals een pre-DPIA) om te bepalen of nieuwe of gewijzigde gegevensverwerkingen een hoog risico kunnen vormen voor de privacy van betrokkenen.
- b) Er is geen systematische beoordeling van alle verwerkingen om te bepalen of deze een hoog risico kunnen opleveren.

2 - Herhaalbaar

2 – Herhaalbaar

- a) Er is een informele procedure voor alle nieuwe en gewijzigde verwerkingen voor het identificeren van hoogrisicoverwerkingen, maar deze wordt niet consequent toegepast of is onvolledig.
- b) Niet alle verwerkingen zijn beoordeeld op een mogelijk hoog risico.
- c) De risicoanalyse die ten grondslag ligt aan de beslissing of een verwerking al dan niet een hoog risico kan opleveren, is niet gedocumenteerd en/of onvolledig.

3 - Bepaald (streefniveau)

3 – Bepaald

- a) Er is een methode/procedure vastgesteld om voor alle nieuwe en gewijzigde verwerkingen te bepalen of deze mogelijk een hoog risico inhouden voor de rechten en vrijheden van betrokkenen.
- b) De methode/procedure om te bepalen of nieuwe en gewijzigde verwerkingen mogelijk een hoog risico vormen voor de rechten en vrijheden van betrokkenen, wordt consequent toegepast.
- c) Alle verwerkingen zijn beoordeeld op mogelijk hoog risico en deze zijn als zodanig aangemerkt in het verwerkingsregister.
- d) De analyse die ten grondslag ligt aan de beslissing of een verwerking een hoog risico kan opleveren, is gedocumenteerd.

4 - Beheerst

4 – Beheerst

- a) Verwerkingen die waarschijnlijk een hoog risico inhouden, worden proactief geïdentificeerd en beheerd.
- b) De procedure voor het identificeren van hoogrisicoverwerkingen wordt periodiek geëvalueerd en zo nodig verbeterd.
- c) De analyse en documentatie van het besluit of een verwerking een hoog risico kan opleveren, is gemakkelijk te vinden en toegankelijk.

5 - Continu verbeteren

5 – Continu verbeteren

- a) Het identificeren van hoog risicoverwerkingen is volledig geïntegreerd in de operationele processen van de organisatie.
- b) Er is een cultuur van voortdurende risicobeoordeling waarbij alle verwerkingen consequent worden beoordeeld op een mogelijk hoog risico en dit wordt aantoonbaar vastgelegd (in het verwerkingsregister).
- c) De documentatie van de analyse en het besluit of een verwerking een hoog risico kan opleveren, is volledig, makkelijk vindbaar, transparant en wordt gezien als een krachtig hulpmiddel binnen de organisatie.

Aan de slag

1. Stel een procedure vast om voor alle nieuwe en gewijzigde verwerkingen te bepalen of deze een hoog risico kunnen inhouden voor de privacy van betrokkenen. Pas deze procedure consequent toe.
2. Beoordeel per verwerking of er een hoog risico is en geef dit vervolgens duidelijk aan in het verwerkingsregister.

Referentie naar andere normen en kaders

AVG Art.35

Link naar relevante IB normen

PR.05 DPIA's

Norm

Indien een verwerking is geïdentificeerd die een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen, wordt een DPIA uitgevoerd die aan de eisen van de AVG voldoet. De organisatie beheert de uitkomsten van DPIA's systematisch.

Waarom is dit nodig?

Om persoonsgegevens adequaat te beschermen moet je verplicht een DPIA uitvoeren voor verwerkingen die een hoog risico kunnen opleveren voor de privacy van betrokkenen. Met een DPIA breng je risico's in kaart en neem je passende maatregelen om deze te verminderen. Zo verklein je de kans op ongeautoriseerde toegang, openbaarmaking van gevoelige informatie en onrechtmatige verwerking.

1 - Ad hoc

1 – Ad hoc

- a) Er is geen formele procedure vastgesteld voor het uitvoeren van DPIA's op nieuwe en sterk gewijzigde verwerkingen die mogelijk een hoog risico inhouden.
- b) De FG wordt (nog) niet betrokken of om advies gevraagd bij het uitvoeren van DPIA's.

2 - Herhaalbaar

2 – Herhaalbaar

- a) Er is een procedure voor het uitvoeren van DPIA's, maar deze wordt niet altijd of niet organisatiebreed toegepast op nieuwe en gewijzigde verwerkingen die mogelijk een hoog risico inhouden.
- b) DPIA-rapporten worden wel opgesteld, maar voldoen niet altijd aan de wettelijke vereisten.
- c) Niet alle hoogrisicoverwerkingen zijn onderworpen aan een DPIA.
- d) De FG wordt betrokken, maar het beslissingsproces over het afwijken van het advies van de FG is niet systematisch gedocumenteerd en is persoonsafhankelijk.

3 - Bepaald (streefniveau)

3 – Bepaald

- a) Er is een vaste methode voor het uitvoeren van DPIA's, en die wordt toegepast op alle nieuwe en sterk gewijzigde verwerkingen die mogelijk een hoog risico inhouden.
- b) Er is een procedure vastgesteld voor het opvolgen (behandelen of accepteren) van risico's die in een DPIA zijn geïdentificeerd.
- c) DPIA-rapporten worden opgesteld volgens een gestandaardiseerd format dat voldoet aan de wettelijke vereisten.
- d) Alle hoogrisicoverwerkingen zijn onderworpen aan een DPIA.
- e) Er is een standaardprocedure voor het documenteren van afwijkingen van het advies van de FG. Deze procedure wordt consequent gevolgd.
- f) De DPIA-rapportages zijn makkelijk vindbaar.

4 - Beheerst

4 – Beheerst

- a) Het uitvoeren van DPIA's en het opvolgen (behandelen of accepteren) van risico's die in een DPIA zijn geïdentificeerd, maakt onderdeel uit van een (organisatiebreed) risicobeheerkader.
- b) DPIA's worden minstens elke 36 maanden opnieuw beoordeeld.
- c) Er is vastgelegd wie mag besluiten dat er van het FG-advies mag worden afgeweken, en deze (tijdelijke) afwijkingen worden actief gemonitord.
- d) In gevallen waar een geïdentificeerd risico niet gemitigeerd of geaccepteerd wordt, wordt dit expliciet

gedocumenteerd en uitgelegd.

- e) Er is een overzicht van en inzicht in de uitgevoerde DPIA's, inclusief de data waarop deze zijn uitgevoerd of herzien.
- f) Periodiek wordt de effectiviteit van de DPIA-procedure geëvalueerd om continue verbetering te bevorderen.

5 - Continu verbeteren

5 – Continu verbeteren

- a) Er is actieve betrokkenheid van het schoolbestuur bij het DPIA-proces, vooral wanneer er wordt afgeweken van het advies van de FG.
- b) De organisatie heeft periodiek overleg met andere organisaties en/of andere samenwerkingsverbanden om te leren van elkaars DPIA's en (de effectiviteit van) mitigerende maatregelen, met name bij soortgelijke verwerkingen.
- c) De organisatie heeft de effectiviteit en efficiëntie van haar DPIA-proces geoptimaliseerd, bijvoorbeeld door gebruik te maken van automatisering of geavanceerde tools.
- d) Bij de overdracht van een project, worden de DPIA en eventuele openstaande maatregelen in acht genomen. Ook wordt er actief naar risico's in de DPIA gevraagd door de betrokken projectmanagementteams.

Aan de slag

1. Stel een procedure vast voor het uitvoeren van DPIA's.
2. Beschrijf in de procedure hoe de risico's die in de DPIA zijn gevonden, worden opgevolgd (mitigeren of accepteren). Beschrijf ook dat afwijkingen van het advies van de FG worden gemotiveerd en geaccordeerd door het schoolbestuur.
3. Voer de procedure uit bij alle nieuwe en sterk gewijzigde verwerkingen die mogelijk een hoog risico inhouden.
4. Hanteer bij het uitvoeren van de DPIA een model dat in de onderwijssector wordt gebruikt en aan de wettelijke eisen voldoet.
5. Zorg ervoor dat de DPIA-rapportages intern makkelijk te raadplegen zijn.

Referentie naar andere normen en kaders

AVG Art.35, Art.36

Link naar relevante IB normen

PR.06 Gegevensbescherming door privacy by design en privacy by default

Norm

Bij de ontwikkeling, het ontwerp, de selectie en het gebruik van toepassingen, diensten en producten houdt de organisatie zo vroeg mogelijk in het proces rekening met de privacybeginselen en privacyrisico's en past gegevensbescherming door ontwerp en standaardinstellingen toe. Toepassingen zijn standaard privacyvriendelijk ingesteld.

Waarom is dit nodig?

Bij de inkoop, de ontwikkeling of het ontwerp van producten, diensten of processen is het belangrijk om in een zo vroeg mogelijk stadium passende waarborgen in te bouwen om de privacy van betrokkenen te beschermen. Dit wordt privacy by design genoemd. Hiermee zorg je ervoor dat je vanaf het begin de beginselen van de AVG naleeft en de rechten van betrokkenen beschermt. Ook voorkom je dat je achteraf aanpassingen moet doen. Daarnaast moeten de standaardinstellingen van een product, dienst of proces op de meest privacyvriendelijke

instelling staan. Dit heet privacy by default. Dit zorgt er bijvoorbeeld voor dat alleen persoonsgegevens worden verzameld die noodzakelijk zijn en dat ze niet langer worden bewaard dan nodig.

1 - Ad hoc

1 – Ad hoc

- a) Bij het ontwerpen, selecteren en gebruiken van toepassingen, diensten en producten wordt er nauwelijks of geen aandacht besteed aan de principes van privacy by design en privacy by default.
- b) Risicomanagement met betrekking tot privacy wordt sporadisch toegepast en stelt weinig tot geen eisen aan externe partijen.

2 - Herhaalbaar

2 – Herhaalbaar

- a) Bij het ontwikkelen, implementeren en gebruiken van toepassingen, diensten en producten is er beperkte aandacht voor de implementatie van zowel privacy by design als privacy by default. De implementatie is gefragmenteerd en/of inconsistent.
- b) Wanneer externe partijen betrokken zijn, wordt er soms, in het kader van risicomanagement, naar hun privacy risicomanagement gevraagd. Maar dit gebeurt niet systematisch of conform de principes van privacy by design.
- c) Toepassingen, diensten en producten zijn soms zodanig geconfigureerd dat alleen de strikt noodzakelijke persoonsgegevens worden verwerkt. Echter, dit gebeurt niet altijd en een begeleidend beleid of documentatie ontbreekt.

3 - Bepaald (streefniveau)

3 – Bepaald

- a) In het kader van risicomanagement hanteert de organisatie gedocumenteerde eisen en beginselen voor privacy by design en privacy by default. Dit omvat de ontwikkeling, het ontwerp, de selectie, en het gebruik van toepassingen, diensten en producten.
- b) Voorafgaand aan de inkoop of de ontwikkeling van toepassingen, diensten en producten vindt systematisch een beoordeling plaats van de privacyrisico's. Hierbij worden de benodigde maatregelen vastgesteld om de privacybeginselen van art. 5 lid 1 AVG na te leven.
- c) Bij samenwerking met externe partijen stelt de organisatie consequent eisen op het gebied van privacy by design.
- d) Privacy by default is consequent geïntegreerd als een standaard aspect van de configuratie voor toepassingen, diensten en producten waarin verwerking met een hoog risico plaatsvindt.
- e) Er zijn gedocumenteerde richtlijnen opgesteld die betrekking hebben op zowel de verwerking als de bescherming van gegevens, waarbij de principes van privacy by default centraal staan.

4 - Beheerst

4 – Beheerst

- a) Privacy by default is consequent geïntegreerd als een standaard aspect van de configuratie voor alle toepassingen, diensten en producten.
- b) De organisatie heeft zowel privacy by design als privacy by default specifiek ingebed in haar processen om privacyrisico's effectief te verminderen en te beheersen. Dit beleid wordt organisatiebreed toegepast.
- c) De organisatie stelt strikte eisen aan externe partijen voor het toepassen van adequaat privacyrisicomanagement. Deze eisen worden periodiek gecontroleerd en, indien nodig, verbeterd.
- d) De privacyrisicobeoordeling is een integraal onderdeel van de ontwikkeling, het ontwerp, de selectie en het gebruik van toepassingen, diensten en producten. Hierbij worden alle toepassingen standaard geconfigureerd om alleen de strikt noodzakelijke persoonsgegevens te verwerken.
- e) Er wordt consequent en periodiek gecontroleerd of de toepassingen, diensten en producten aan deze privacystandaarden voldoen. Afwijkingen van het beleid worden direct gecorrigeerd en/of gedocumenteerd volgens het principe "pas toe of leg uit".

5 - Continu verbeteren

5 – Continu verbeteren

- a) De organisatie past haar processen proactief aan bij nieuwe/gewijzigde risico's. Deze aanpassingen kunnen voortkomen uit informatie verkregen door risicobeoordeling, gewijzigde inzichten naar aanleiding van de evaluatie van een datalek, wijzigingen in wet- en regelgeving, of andere relevante factoren. Bij deze updates worden de principes van zowel privacy by design als privacy by default consequent toegepast.
- b) Strikte eisen met betrekking tot privacyrisicomanagement, zowel voor privacy by design als privacy by default, zijn verankerd in de contractuele relaties van de organisatie.
- c) Het beleid voor privacy by default, in het bijzonder het minimaliseren van gegevensverwerking, wordt consequent toegepast in alle nieuwe en bestaande toepassingen, processen en systemen. Hierbij wordt proactief geanticipeerd op en gereageerd op veranderingen in het privacylandschap.

Aan de slag

1. Leg eisen vast voor het toepassen van privacy by design en privacy by default.
2. Zorg voor een systematische beoordeling van privacyrisico's voor de inkoop of de ontwikkeling van toepassingen, diensten en producten.
3. Pas de eisen op het gebied van privacy by design en privacy by default toe bij samenwerking met externe partijen en bij inkoop van software van verwerkers (leveranciers).
4. Zorg ervoor dat bij toepassingen, software en producten waarin verwerking met een hoog risico plaatsvindt privacy by default consequent is geïntegreerd als een standaard aspect van de configuratie.

Referentie naar andere normen en kaders

AVG Art.25

Link naar relevante IB normen

SD.01

PR.07 Bewaar- en vernietigingsbeleid

Norm

Persoonsgegevens worden tijdig verwijderd of geanonimiseerd.

Waarom is dit nodig?

Met een adequaat en consequent uitgevoerd bewaar- en vernietigingsbeleid zorg je ervoor dat je school persoonsgegevens tijdig anonimiseert of verwijdert. Hierdoor bescherm je de persoonsgegevens beter en voorkom je dat onnodig bewaarde persoonsgegevens kunnen worden verwerkt voor andere dan de oorspronkelijke doelen of door een datalek in verkeerde handen komen.

1 - Ad hoc

1 – Ad hoc

- a) Er is geen vastgesteld beleid voor het verwijderen en anonimiseren van gegevens ('bewaarbeleid' of 'vernietigingsbeleid').
- b) Het verwijderen of anonimiseren van persoonsgegevens gebeurt niet, onregelmatig en/of inconsistent (bijvoorbeeld afhankelijk van individuen of incidenten).

2 - Herhaalbaar

2 – Herhaalbaar

- a) Er is informeel beleid of beleid op decentraal niveau voor het verwijderen en/of anonimiseren van gegevens.
- b) Voor algemene, veelvoorkomende gevallen zijn er procedures voor het verwijderen van gegevens, maar voor meer specifieke gevallen ontbreken deze procedures.

3 - Bepaald (streefniveau)

3 – Bepaald

- a) Er is beleid vastgesteld voor het verwijderen en/of anonimiseren van gegevens.
- b) De processen om persoonsgegevens te verwijderen of te anonimiseren zijn gedocumenteerd.
- c) Persoonsgegevens die niet meer nodig zijn worden tijdig verwijderd of geanonimiseerd, conform het beleid.
- d) Waar noodzakelijk zijn specifieke procedures vastgesteld voor het verwijderen van gegevens. Hierin is vastgesteld wat de toepasselijke bewaartermijn is en op welke wijze verwijdering plaats dient te vinden.
- e) Het beleid en de procedures voor het verwijderen en anonimiseren van gegevens worden consequent toegepast.

4 - Beheerst

4 – Beheerst

- a) Het beleid en de procedures voor het verwijderen en anonimiseren worden periodiek geëvalueerd en zo nodig aangepast.
- b) Het beleid besteedt aandacht aan het verwijderen/anonimiseren bij leveranciers (bijvoorbeeld SaaS-applicaties of applicaties die anderszins persoonsgegevens verwerken).
- c) Periodiek wordt gecontroleerd of applicaties daadwerkelijk verwijderen of anonimiseren conform het bewaar- en vernietigingsbeleid.
- d) Waar mogelijk wordt het verwijderen of anonimiseren van persoonsgegevens geautomatiseerd uitgevoerd.

5 - Continu verbeteren

5 – Continu verbeteren

- a) Het beleid en de procedures voor het verwijderen en anonimiseren van gegevens zijn volledig, transparant, en worden gezien als krachtige hulpmiddelen binnen de organisatie.
- b) Het is mogelijk een geautomatiseerd bewaar- en vernietigingsregime toe te passen op persoonsgegevens, bij voorkeur ook gekoppeld aan doelen.
- c) Deze geautomatiseerde systemen zijn volledig geïntegreerd in de operationele processen van de organisatie.

Aan de slag

1. Stel een bewaartermijnenbeleid op. Leg daarin de bewaartermijnen vast en neem hierin ook de bewaartermijnen op van persoonsgegevens die worden verwerkt bij leveranciers.
2. Neem in het beleid criteria op voor het verwijderen of anonimiseren van persoonsgegevens die niet meer nodig zijn.
3. Stel een procedure vast voor het verwijderen van gegevens en neem hierin op wie welke gegevens verwijdert en wanneer. Zorg ervoor dat deze procedure op tijd en consequent wordt toegepast.

Referentie naar andere normen en kaders

AVG Art.5 lid 1 sub e

Link naar relevante IB normen

DM.01, DM.02, DM.04, DM.06

3. Organisatorische inbedding

Om privacy goed te regelen binnen je school is het belangrijk om over de juiste privacykennis te beschikken en het toezicht op de verwerking van persoonsgegevens goed te regelen via de Functionaris Gegevensbescherming (FG) en (G)MR. Medewerkers moeten worden getraind om veilig en verantwoord om te gaan met persoonsgegevens en ict, en weten bij wie zij terecht kunnen met vragen over privacy.

Wie is verantwoordelijk:

Eindverantwoordelijk: Schoolbestuur

Verantwoordelijk voor de uitvoering: Privacy Officer of IBP-adviseur, FG

Geïnformeerd: (G)MR, medewerkers

OI.01 Aanwijzing en positie Functionaris Gegevensbescherming

Norm

De organisatie heeft een Functionaris Gegevensbescherming (FG) aangesteld en zodanig onafhankelijk gepositioneerd dat deze effectief toezicht kan houden.

Waarom is dit nodig?

De FG kan zijn toezichthoudende en adviserende taken effectief en onafhankelijk uitvoeren als zijn rol binnen de organisatie correct en volledig is ingebed. Hierdoor is het schoolbestuur beter in staat om de rechten en vrijheden van leerlingen, ouders, medewerkers en andere betrokkenen te waarborgen. Dit draagt verder bij aan het bewustzijn en de kennis binnen de school om persoonsgegevens conform de AVG te verwerken.

1 - Ad hoc

1 – Ad hoc

- a) Er is geen FG aangesteld of de aangewezen FG heeft onvoldoende middelen, tijd of ondersteuning voor het effectief uitvoeren van zijn of haar wettelijke taken.
- b) De rol en verantwoordelijkheden van de FG zijn niet gedefinieerd.
- c) De contactgegevens van de FG ontbreken en zijn niet (makkelijk) vindbaar.
- d) De FG is niet betrokken bij opleiding en bewustwordingsprogramma's.

2 - Herhaalbaar

2 – Herhaalbaar

- a) Een FG is aangesteld, maar de taken van de FG zijn niet duidelijk omschreven en/of de rol van de FG is niet onafhankelijk (genoeg) gepositioneerd in de organisatie.
- b) De FG heeft beperkte tijd, middelen of ondersteuning (van het management) om zijn of haar taken te vervullen.
- c) De betrokkenheid van de FG bij opleiding en bewustwordingsprogramma's is minimaal en/of gebeurt ad hoc.

3 - Bepaald (streefniveau)

3 – Bepaald

- a) De taken en verantwoordelijkheden van de FG zijn duidelijk omschreven en de FG is onafhankelijk gepositioneerd binnen de organisatie. De FG ontvangt geen instructies met betrekking tot de uitvoering van zijn of haar taken.
- b) De FG heeft geen taken of verplichtingen die kunnen leiden tot een belangenconflict bij de uitvoering van zijn of haar taken als FG.
- c) De FG heeft voldoende tijd en middelen om zijn of haar taken effectief uit te voeren.
- d) Het proces voor het aannemen van een FG en het functieprofiel van de FG voldoen aan de eisen gesteld in

artikel 37 lid 5 van de AVG.

- e) De FG wordt tijdig betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens, waaronder advies bij iedere DPIA.
- f) Contactgegevens van de FG zijn actueel, beschikbaar, en makkelijk te vinden.
- g) De FG is betrokken bij opleiding en bewustwordingsprogramma's op het gebied van privacy.
- h) De FG stemt periodiek af met het schoolbestuur binnen de organisatie.
- i) De FG brengt rechtstreeks verslag uit aan het schoolbestuur over de naleving van de AVG door de organisatie.

4 - Beheerst

4 – Beheerst

- a) De organisatie heeft een gedocumenteerd proces om de aanstelling en het functioneren van de FG te waarborgen. Dit document bevat onder meer:
 - 1. Een duidelijke beschrijving dat de FG afstemt met het schoolbestuur, inclusief details over hoe en met welke frequentie deze afstemming plaatsvindt.
 - 2. Een uitgewerkte rolbeschrijving met daarin een heldere beschrijving van de bevoegdheden, rechten (waaronder ontslagbescherming) en plichten van de FG.
- b) De FG voert periodiek zelfevaluatie uit en betreft het management bij het verfijnen van de rol en positie van de FG. Indien uit de evaluatie blijkt dat taken onduidelijk zijn of de rol niet goed is gepositioneerd, betreft de FG het management om samen tot een oplossing te komen.
- c) De contactgegevens van de FG zijn niet alleen beschikbaar, maar worden ook proactief gecommuniceerd naar relevante partijen.
- d) De FG brengt periodiek verslag uit aan het schoolbestuur over de naleving van de AVG door de organisatie.

5 - Continu verbeteren

5 – Continu verbeteren

- a) Het schoolbestuur neemt proactief het initiatief om de stand van zaken met betrekking tot de bescherming van persoonsgegevens in de organisatie, inclusief audits, met de FG te bespreken.
- b) De FG brengt regelmatig ongevraagd advies uit; het schoolbestuur past deze adviezen toe of legt vast waarom daarvan afgeweken wordt.
- c) De aanstelling, verantwoordelijkheden, en middelen voor de FG zijn optimaal en worden continu verbeterd.
- d) De FG speelt een strategische rol in het ontwikkelen en leveren van opleiding en bewustwordingsprogramma's.
- e) De FG is betrokken bij opleiding en bewustwordingsprogramma's op het gebied van informatiebeveiliging en privacy.

Aan de slag

- 1. Wijs een Functionaris voor Gegevensbescherming (FG) aan. Zorg dat het functieprofiel voldoet aan de eisen uit artikel 37 lid 5 van de AVG.
- 2. Omschrijf de taken en verantwoordelijkheden van de FG in een beleid, werkwijze, procedure of reglement.
- 3. Positioneer de FG onafhankelijk binnen de organisatie. Zorg ervoor dat de FG geen taken of verplichtingen heeft die kunnen leiden tot een belangenconflict bij de uitvoering van zijn taken als FG.
- 4. Zorg ervoor dat de FG geen instructies met betrekking tot de uitvoering van zijn of haar taken ontvangt.
- 5. Stel voor de FG voldoende tijd en middelen beschikbaar om zijn of haar taken effectief uit te voeren.
- 6. Betrek de FG tijdig betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens waaronder advies bij iedere DPIA.
- 7. Zorg ervoor dat de contactgegevens van de FG actueel, publiek beschikbaar en makkelijk te vinden zijn. Bijvoorbeeld via de publieke website van het schoolbestuur.

8. Betrek de FG bij opleiding en bewustwordingsprogramma's op het gebied van privacy.
9. Stem als schoolbestuur periodiek af met de FG.
10. Laat de FG – ten minste jaarlijks – verslag uitbrengen aan het schoolbestuur over de naleving van de AVG door de organisatie.

Referentie naar andere normen en kaders

AVG Art.37, Art.38, Art.39

Link naar relevante IB normen

OI.02 Privacyorganisatie

Norm

Er is – naast de FG – ruime (juridische) kennis en ervaring binnen de organisatie beschikbaar over bescherming van persoonsgegevens en relevante wet- en regelgeving.

Waarom is dit nodig?

Als er binnen de school voldoende (juridische) kennis is van privacy ben je beter in staat om de juiste beslissingen te nemen om conform de AVG persoonsgegevens te verwerken van leerlingen, medewerkers en anderen. Daarmee verklein je het risico op onrechtmatige verwerkingen en beveiligingsincidenten.

1 - Ad hoc

1 – Ad hoc

- a) Er is geen of weinig (juridische) kennis over privacy.
- b) Er is geen aanvullende privacyfunctionaris (of andere privacydeskundige) naast de FG.

2 - Herhaalbaar

2 – Herhaalbaar

- a) Er zijn één of enkele Privacy Officers (of adviseurs) die actief bijdragen aan het oplossen van (complexe) vraagstukken over privacy en de bescherming van persoonsgegevens.
- b) Er is incidenteel en/of informeel overleg en afstemming tussen de privacy- en informatiebeveiligingsfunctionarissen.

3 - Bepaald (streefniveau)

3 – Bepaald

- a) Er is een (virtueel) privacyteam waarbij de FG, Privacy Officer(s) en eventuele decentrale privacyambassadeurs/-coördinatoren zijn aangesloten.
- b) Het privacyteam werkt nauw samen met de informatiebeveiligingsfunctionarissen om vraagstukken rond informatiebeveiliging zoveel mogelijk gezamenlijk of althans in overleg, op te lossen.
- c) Medewerkers kunnen eenvoudig en makkelijk contact opnemen met het privacyteam. Het privacyteam reageert binnen een vooraf vastgestelde maximale reactietijd op vragen uit de organisatie.
- d) Het privacyteam heeft periodiek overleg om de werkzaamheden te bespreken en activiteiten af te stemmen, met betrokkenheid van relevante stakeholders.

4 - Beheerst

4 – Beheerst

- a) Privacy Officer(s) en eventuele decentrale privacyambassadeurs/-coördinatoren evalueren periodiek de

privacygerelateerde werkzaamheden binnen de organisatie. De FG kan hier ook over adviseren. Daar waar nodig worden verbeteringen doorgevoerd.

5 - Continu verbeteren

5 – Continu verbeteren

- a) Het initiatief tot verbeteringen van de privacygerelateerde werkzaamheden binnen de organisatie komt van de teams, afdelingen of het schoolbestuur zelf in plaats van de privacyfunctionarissen.
- b) Organisatieonderdelen beschikken met betrekking tot de diensten die zij leveren over uitgebreide (juridische) kennis en ervaring over bescherming van persoonsgegevens en relevante wet- en regelgeving.
- c) Privacyfunctionarissen werken proactief samen met andere stakeholders voor de continue verbetering van de privacygerelateerde werkzaamheden.

Aan de slag

- 1. Richt een (virtueel) privacyteam in waarbij de FG, Privacy Officer(s) en eventuele decentrale privacy ambassadeurs/coördinatoren zijn aangesloten.
- 2. Zorg ervoor dat dit privacyteam nauw samenwerkt met de informatiebeveiligingsfunctionarissen om vraagstukken waarbij informatiebeveiliging speelt zoveel mogelijk gezamenlijk en in overleg op te lossen.
- 3. Zorg ervoor dat medewerkers van de organisatie eenvoudig en makkelijk contact kunnen opnemen met het privacyteam en dat het privacyteam reageert binnen een vooraf vastgestelde tijd op vragen uit de organisatie.
- 4. Zorg ervoor dat het privacyteam periodiek overlegt om de werkzaamheden te bespreken en activiteiten af te stemmen met stakeholders.

Referentie naar andere normen en kaders

AVG Art.24 lid 1

Link naar relevante IB normen

OI.03 Betrokkenheid medezeggenschap

Norm

De medezeggenschapsraad (MR) wordt geïnformeerd en betrokken bij de omgang met en de bescherming van persoonsgegevens van medewerkers en leerlingen.

Waarom is dit nodig?

Door de medezeggenschapsraad te betrekken bij besluiten over regelingen en procedures over de bescherming van persoonsgegevens, vergroot je het draagvlak hiervoor binnen de school. Daarnaast draagt betrokkenheid van de medezeggenschapsraad bij aan de kwaliteit van de besluiten die jouw school neemt.

1 - Ad hoc

1 – Ad hoc

- a) De medezeggenschapsraad wordt niet of slechts informeel betrokken bij onderwerpen over de omgang met en bescherming van persoonsgegevens.

2 - Herhaalbaar

2 – Herhaalbaar

- a) De medezeggenschapsraad wordt ad hoc betrokken bij onderwerpen over de omgang met en bescherming

van persoonsgegevens.

b) De informatievoorziening aan de medezeggenschapsraad is willekeurig en ongestructureerd.

3 - Bepaald (streefniveau)

3 – Bepaald

a) Er is een gedocumenteerd proces dat specificeert hoe en wanneer de medezeggenschapsraad geïnformeerd en betrokken wordt bij wettelijke taken op het gebied van privacy.

b) Instemmingsprocedures zijn duidelijk gedocumenteerd en worden gevolgd waar wettelijk vereist.

4 - Beheerst

4 – Beheerst

a) De medezeggenschapsraad wordt actief geïnformeerd en betrokken bij onderwerpen over de omgang met en bescherming van persoonsgegevens van medewerkers en andere relevante groepen binnen hun mandaat.

b) De effectiviteit van de instemmingsprocedures en communicatie daaromheen worden periodiek geëvalueerd en waar nodig aangepast.

5 - Continu verbeteren

5 – Continu verbeteren

a) Er is een breed bewustzijn in de organisatie over de rol van de medezeggenschapsraad in de omgang met en bescherming van persoonsgegevens, en over de rol van overige relevante doelgroepen voor zover deze tot het mandaat van de medezeggenschapsraad behoren.

b) De medezeggenschapsraad is proactief betrokken, zowel op verzoek als ongevraagd, bij onderwerpen met betrekking tot de omgang met en bescherming van persoonsgegevens van medewerkers en andere relevante groepen binnen hun mandaat.

c) De privacyaansprekpunten in de organisatie en de medezeggenschapsraad weten elkaar makkelijk te bereiken. Hier wordt bijvoorbeeld aandacht aan gegeven in o.a. privacy awareness-trainingen en de rol van de medezeggenschapsraad.

Aan de slag

1. Stel een proces op voor hoe en wanneer de medezeggenschapsraad geïnformeerd en betrokken wordt bij wettelijke taken op het gebied van privacy.

2. Leg in het IBP-beleid vast wanneer en hoe de medezeggenschapsraad om instemming wordt gevraagd.

Referentie naar andere normen en kaders

AVG Art.24 en Wet medezeggenschap scholen (WMS)

Link naar relevante IB normen

OI.04 Bewustwording bescherming persoonsgegevens

Norm

Medewerkers en leerlingen worden bewust gemaakt van privacygerelateerde kwesties en hun verantwoordelijkheden met betrekking tot het beschermen van persoonsgegevens. Ook zijn er voldoende middelen beschikbaar om medewerkers te trainen.

Waarom is dit nodig?

Als medewerkers en leerlingen zich bewust zijn van het belang van een zorgvuldige omgang met en bescherming van hun eigen persoonsgegevens en die van anderen, zullen ze daar eerder naar handelen. Dat verkleint dat de kans op onrechtmatige verwerking, verlies of misbruik van persoonsgegevens.

1 - Ad hoc

1 – Ad hoc

- a) Er zijn geen activiteiten of initiatieven gedefinieerd of uitgevoerd om het bewustzijn over privacy te vergroten. Medewerkers worden bij indiensttreding niet geïnformeerd over privacy.
- b) Leerlingen worden niet geïnformeerd over het belang van privacy en de bescherming van persoonsgegevens.

2 - Herhaalbaar

2 – Herhaalbaar

- a) Er zijn activiteiten of initiatieven gedefinieerd om het bewustzijn over privacy te vergroten, maar deze worden informeel uitgevoerd (alleen op verzoek of als reactie op een geïdentificeerde behoefte, bijvoorbeeld naar aanleiding van een incident).
- b) Leerlingen worden op incidentele basis geïnformeerd over het belang van privacy en de bescherming van persoonsgegevens.

3 - Bepaald (streefniveau)

3 – Bepaald

- a) Er is een programma/opleidingsplan waarin medewerkers bij indiensttreding en tijdens het dienstverband worden geïnformeerd over privacy en de bescherming van persoonsgegevens.
- b) Medewerkers zijn goed geïnformeerd over hun verantwoordelijkheden met betrekking tot privacy en de bescherming van persoonsgegevens en handelen daarnaar.
- c) Leerlingen worden op een planmatige manier geïnformeerd over het belang van privacy en de bescherming van persoonsgegevens.

4 - Beheerst

4 – Beheerst

- a) Voor alle bewustwordingsniveaus worden de vaardigheidsvereisten systematisch bijgehouden; deskundigheidsbevordering is gewaarborgd in alle kritieke gebieden en certificering op het gebied van privacyskills wordt aangemoedigd.
- b) Periodiek wordt geëvalueerd of met de trainingen de beoogde resultaten worden behaald en waar nodig worden trainingen en/of het trainingsprogramma aangepast.
- c) Medewerkers en ingehuurd medewerkers hebben aantoonbaar een passende (bewustwordings)training of instructie gevolgd over hun verantwoordelijkheden met betrekking tot de bescherming van persoonsgegevens.

5 - Continu verbeteren

5 – Continu verbeteren

- a) Er is een formeel proces dat zich richt op voortdurende vaardigheidsverbetering, gebaseerd op heldere persoonlijke en organisatiebrede doelen, waarbij medewerkers en leerlingen geïnformeerd worden over relevante privacygerelateerde kwesties.
- b) Privacybewustzijn en de bescherming van persoonsgegevens zijn volledig geïntegreerd in alle aspecten van de organisatie, met volledige betrokkenheid en participatie van alle medewerkers, inclusief het schoolbestuur.
- c) Leerlingen worden consequent geïnformeerd over het belang van privacy en de bescherming van persoonsgegevens. Deze informatie is geïntegreerd in het onderwijsprogramma, waarbij leerlingen actief betrokken zijn en participeren.

Aan de slag

1. Neemt het bewust maken van medewerkers en leerlingen over het belang van privacy en de bescherming van persoonsgegevens en hun eigen verantwoordelijkheden op dat vlak op in beleid.
2. Stel een bewustwordingsprogramma of opleidingsplan op om medewerkers te informeren over privacy en de bescherming van persoonsgegevens. Zorg ervoor dat medewerkers hier minstens een keer per jaar aan

deelnemen.

3. Informeer medewerkers over hun verantwoordelijkheden met betrekking tot privacy en de bescherming van persoonsgegevens.
4. Informeer leerlingen over het belang van privacy en de bescherming van persoonsgegevens en neem dit op in het onderwijsprogramma.

Referentie naar andere normen en kaders

AVG Art.24 lid 1

Link naar relevante IB normen

HR.06

4. Rechten van betrokkenen

Leerlingen, ouders en medewerkers hebben bepaalde rechten bij de verwerking van hun persoonsgegevens. Je school moet hen hierin faciliteren. Het is belangrijk dat betrokkenen worden geïnformeerd over de verwerking van hun persoonsgegevens en hoe zij hun rechten kunnen uitoefenen. Je organisatie moet een procedure hebben die ervoor zorgt dat je de verzoeken van betrokkenen tijdig en op de juiste wijze kunt afhandelen.

Wie is verantwoordelijk:

Eindverantwoordelijk: Schoolbestuur

Verantwoordelijk voor de uitvoering: Privacy Officer of IBP-adviseur

Geraadpleegd: Proceseigenaar, Verwerker, FG

Geïnformeerd: Verwerker, medewerkers

RB.01 Afhandeling rechten van betrokkenen

Norm

De organisatie heeft een procedure voor de afhandeling van rechten van betrokkenen waarin de technische en organisatorische maatregelen zijn vastgelegd en wie verantwoordelijk is om deze uit te voeren.

Waarom is dit nodig?

Passende procedures zijn voor de afhandeling van de rechten van betrokkenen dragen bij aan een efficiënte en nauwkeurige verwerking van verzoeken binnen de wettelijke termijn. Leerlingen en medewerkers mogen van een school verwachten dat hun verzoeken adequaat worden afgehandeld en dat er helder wordt gecommuniceerd over hun rechten. Dit vergroot hun gevoel van veiligheid, vertrouwen en kwaliteit over je school.

1 - Ad hoc

1 – Ad hoc

- a) De organisatie heeft geen technische of organisatorische maatregelen genomen om de rechten van betrokkenen te waarborgen.
- b) Er is geen proces voor het indienen en afhandelen van verzoeken.
- c) Medewerkers herkennen AVG-verzoeken niet en weten niet naar wie ze deze moeten doorsturen voor afhandeling.
- d) De organisatie houdt geen registratie bij van eerder behandelde verzoeken. Er bestaat geen procedure om, ten behoeve van consistentie en de waarborg van rechtsgelijkheid, nieuwe verzoeken te toetsen aan de hand van eerder afgehandelde verzoeken.

2 - Herhaalbaar

2 – Herhaalbaar

- a) De organisatie heeft voor de afhandeling van rechten van betrokkenen enkele technische en organisatorische maatregelen genomen, maar de implementatie is onvolledig en inconsistent.
- b) Verzoeken kunnen zowel analoog als digitaal worden ingediend, maar de communicatie hierover is gebrekkig.
- c) Er zijn basisprocedures voor de afhandeling van verzoeken, maar de naleving van termijnen is inconsistent en/of de communicatie met betrokkenen is gebrekkig.
- d) Er is een registratie van eerder behandelde verzoeken, maar deze wordt niet consequent gebruikt om, ten behoeve van consistentie en de waarborg van rechtsgelijkheid, nieuwe verzoeken te toetsen.

3 - Bepaald (streefniveau)

3 – Bepaald

- a) Er is een procedure voor de afhandeling van verzoeken van betrokkenen vastgesteld, waarin ten minste het volgende is opgenomen:
 - op welke wijze verzoeken kunnen worden ingediend
 - op welke wijze de identiteit van verzoeker wordt vastgesteld
 - wie verantwoordelijk is voor de afhandeling
 - de toepasselijke termijnen
 - de criteria voor het toewijzen en afwijzen van een verzoek
 - het informeren van ontvangers over een verzoek.
- b) Verzoeken kunnen zowel analoog als digitaal worden ingediend en dit proces is duidelijk gecommuniceerd naar betrokkenen.
- c) Betrokkenen ontvangen altijd een ontvangstbevestiging van hun verzoeken en worden tijdig geïnformeerd over de status van de behandeling.
- d) Applicaties en systemen bevatten voldoende mogelijkheden om de rechten van betrokkenen effectief uit te voeren.
- e) Er is een registratie van eerder behandelde verzoeken die consequent wordt bijgehouden en gebruikt om nieuwe verzoeken te beoordelen, met als doel de rechtsgelijkheid te waarborgen.
- f) Medewerkers zijn goed getraind in het herkennen van AVG-verzoeken en weten precies naar wie ze deze moeten doorsturen.

4 - Beheerst

4 – Beheerst

- a) Verzoeken van betrokkenen worden tijdig afgehandeld en er is een proces voor het signaleren, melden en analyseren van vertragingen.
- b) Er is een duidelijke procedure voor de afhandeling van verzoeken, inclusief monitoring en verbetering van de reactietijden. Dit wordt periodiek geanalyseerd om verbetermaatregelen te treffen.
- c) De organisatie houdt een gedetailleerde registratie bij van eerder behandelde verzoeken en gebruikt deze om nieuwe verzoeken consistent en nauwkeurig te toetsen.

5 - Continu verbeteren

5 – Continu verbeteren

- a) Alle applicaties en systemen bevatten geavanceerde en effectieve mogelijkheden voor de uitvoering van de rechten van betrokkenen.
- b) Er worden benchmarks uitgevoerd (bijvoorbeeld binnen de onderwijssector) om te toetsen of de uitvoering van rechten van betrokkenen aansluit op wat algemeen gangbaar is.

Aan de slag

1. Stel een procedure vast voor de afhandeling van rechten betrokkenen. Beschrijf in deze procedure hoe iemand een verzoek kan indienen, hoe de identiteit van de verzoeker wordt vastgesteld, wie verantwoordelijk is voor de afhandeling, welke termijnen er gelden en wat de criteria voor toe- en

afwijzing zijn. Neem in de procedure ook op hoe andere partijen die persoonsgegevens hebben ontvangen - bijvoorbeeld verwerkers - worden geïnformeerd over toegewezen verzoeken tot rectificatie, verwijdering of beperking. Communiceer duidelijk naar de betrokkenen hoe verzoeken - digitaal en analoog - kunnen worden ingediend.

2. Informeer betrokkenen over de status en afhandeling en van hun verzoek.
3. Maak inzichtelijk of en hoe applicaties en systemen die worden gebruikt mogelijkheden bevatten om aan verzoeken van betrokkenen te kunnen voldoen.
4. Hou een centraal register bij van alle ingekomen en afgehandelde verzoeken.
5. Zorg ervoor dat medewerkers AVG-verzoeken herkennen en weten aan wie deze moeten worden doorgestuurd.

Referentie naar andere normen en kaders

AVG Art.12, Art. 15, Art.16, Art.17, Art.18, Art.19, Art.21

Link naar relevante IB normen

RB.02 Informatieplicht

Norm

Betrokkenen worden, zoveel als mogelijk, voorafgaand aan een verwerking op de hoogte gesteld van de wettelijk vereiste informatie over de verwerking van hun persoonsgegevens.

Waarom is dit nodig?

Door vooraf duidelijk te informeren over de verwerking van persoonsgegevens, weten leerlingen en medewerkers welke gegevens je over hen verwerkt en hoe en waarom je dat doet. Met deze informatie kunnen zij hun rechten uitoefenen. Bovendien laat je hiermee als school zien dat je persoonsgegevens op een behoorlijke en transparante manier verwerkt.

1 - Ad hoc

1 – Ad hoc

- a) Betrokkenen worden niet of onvoldoende geïnformeerd over de verwerking van hun persoonsgegevens, alsmede hun rechten.
- b) Er is geen informatie verstrekt aan betrokkenen van wie de persoonsgegevens niet rechtstreeks zijn verkregen.
- c) De organisatie heeft geen algemene privacyverklaring gepubliceerd op de website of in applicaties en formulieren.
- d) Er is geen cookiebeleid of uniforme afspraken over de toepassing van cookies.
- e) Bezoekers van de website worden niet geïnformeerd over het gebruik van cookies.

2 - Herhaalbaar

2 – Herhaalbaar

- a) Betrokkenen worden geïnformeerd, maar de communicatie is soms niet adequaat of te laat.
- b) Er is een algemene privacyverklaring, maar deze is mogelijk niet volledig of niet up-to-date, en is niet in eenvoudige en duidelijke op de doelgroep gerichte taal opgeschreven.
- c) De informatie over de verwerking van persoonsgegevens in applicaties en formulieren is beperkt en niet altijd duidelijk.
- d) Betrokkenen van wie de persoonsgegevens niet rechtstreeks zijn verkregen, worden niet altijd of niet volledig

geïnformeerd.

e) Er zijn informele afspraken over het gebruik van cookies, maar deze voldoen niet (volledig) aan wet- en regelgeving en/of worden niet consequent geïmplementeerd.

3 - Bepaald (streefniveau)

3 – Bepaald

a) Er is beleid vastgesteld over het informeren van betrokkenen, inclusief de timing van de informatieverstrekking.

b) Betrokkenen worden adequaat en tijdig geïnformeerd in overeenstemming met de beginselen van behoorlijke en transparante verwerking.

c) Personen van wie de persoonsgegevens niet rechtstreeks zijn verkregen, worden binnen een maand geïnformeerd.

d) De organisatie heeft een privacyverklaring op de algemene website in eenvoudige en duidelijke taal (taalniveau B1) en een verwijzing in applicaties en formulieren waar verwerkingen plaatsvinden.

e) Er is cookiebeleid vastgelegd en dit voldoet aan wet- en regelgeving.

f) De website informeert gebruikers over het cookiebeleid.

4 - Beheerst

4 – Beheerst

a) Er wordt periodiek geëvalueerd of de procedures voor het informeren van betrokkenen adequaat zijn en worden nagekomen. Daar waar nodig worden aanpassingen doorgevoerd.

b) De privacyverklaring is up-to-date en de inhoud wordt afgestemd op de specifieke context van applicaties en formulieren.

c) Het cookiebeleid en de implementatie ervan worden periodiek geëvalueerd. Daar waar nodig worden aanpassingen doorgevoerd.

5 - Continu verbeteren

5 – Continu verbeteren

a) Transparantie wordt beschouwd als een kwaliteitsaspect en een kans voor de organisatie om aan te tonen hoe zorgvuldig ze omgaat met persoonsgegevens van leerlingen, medewerkers en overige betrokkenen. Er is bijvoorbeeld een online gepubliceerd verwerkingsregister.

b) Applicaties en formulieren bieden uitgebreide uitleg over de verwerking van persoonsgegevens.

c) Er is een proactieve benadering om de gebruikerservaring van de website met betrekking tot de bescherming van persoonsgegevens te verbeteren, inclusief een transparant en begrijpelijk cookiebeleid.

d) Het cookiebeleid en de implementatie ervan worden proactief getoetst aan de nieuwste inzichten en richtlijnen.

Aan de slag

1. Leg – bijvoorbeeld als onderdeel van het IBP-beleid – vast hoe en wanneer betrokkenen worden geïnformeerd over de verwerking van hun persoonsgegevens.

2. Leg in een privacyreglement vast wat de rechten en verplichtingen zijn van de betrokkenen en het schoolbestuur met betrekking tot de verwerking van persoonsgegevens. Neem op de website en in de schoolgids een leesbare samenvatting op van dit privacyreglement in de vorm van een privacyverklaring.

3. Stel het privacyreglement, de privacyverklaring en communicatie over rechten van betrokkenen op in duidelijke en eenvoudige taal afgestemd op de doelgroep.

4. Zorg ervoor dat op plaatsen waar persoonsgegevens worden verzameld - bijvoorbeeld applicaties en formulieren - een duidelijke verwijzing staat naar de privacyverklaring.

5. Informeer bezoekers van de website over het cookiebeleid met een cookiemelding.

Referentie naar andere normen en kaders

AVG Art.12, Art.13 en Art.14

Link naar relevante IB normen

RB.03 Toestemming

Norm

De organisatie voldoet aan de wettelijke vereisten wanneer een verwerking is gebaseerd op toestemming.

Waarom is dit nodig?

Door bij de verwerking van persoonsgegevens gebaseerd op de verwerkingsgrondslag ‘toestemming’ aan de voorwaarden van de AVG te voldoen zorg je ervoor dat betrokkenen als leerlingen en medewerkers geïnformeerd zijn, in vrijheid hun toestemming kunnen geven en weten zij dat zij die ook kunnen weigeren en intrekken. Alleen dan is de toestemming geldig en kun je de persoonsgegevens rechtmatig verwerken.

1 - Ad hoc

1 – Ad hoc

- a) Er zijn geen gestandaardiseerde processen voor de identificatie van verwerkingen die op toestemming zijn gebaseerd.
- b) Er is geen documentatie van toestemming.
- c) Er is geen procedure om toestemming in te trekken.

2 - Herhaalbaar

2 – Herhaalbaar

- a) De organisatie heeft een informeel proces om verwerkingen die op toestemming zijn gebaseerd te identificeren, maar dit proces wordt niet consequent gevolgd.
- b) De organisatie vraagt toestemming van betrokkenen, maar de toestemming is niet altijd vrij, geïnformeerd, specifiek en ondubbelzinnig.
- c) Toestemming wordt in een aantal gevallen gedocumenteerd, maar dit is nog niet consequent of volledig.
- d) Betrokkenen hebben de mogelijkheid om toestemming in te trekken, maar dit proces is niet altijd duidelijk of gemakkelijk.

3 - Bepaald (streefniveau)

3 – Bepaald

- a) De organisatie heeft vastgesteld welke verwerkingen op toestemming zijn gebaseerd.
- b) Toestemming wordt correct gevraagd volgens de vereisten die zijn opgenomen in AVG artikel 4 sub 11 alsmede artikel 7 en 8 AVG.
- c) Toestemming wordt consequent en volledig gedocumenteerd.
- d) Betrokkenen kunnen hun toestemming gemakkelijk intrekken.

4 - Beheerst

4 – Beheerst

- a) De organisatie evalueert periodiek haar processen om te bepalen welke verwerkingen op toestemming zijn gebaseerd.
- b) Er zijn periodieke beoordelingen en audits om ervoor te zorgen dat toestemming correct wordt gevraagd en gedocumenteerd.
- c) Het proces voor het intrekken van toestemming wordt periodiek geëvalueerd en indien nodig aangepast.

5 - Continu verbeteren

5 – Continu verbeteren

- a) De organisatie heeft systemen en processen om te bepalen welke verwerkingen op toestemming zijn gebaseerd.
- b) Documentatie van toestemming wordt (automatisch) bijgewerkt en gevolgd via systemen.
- c) Betrokkenen kunnen hun toestemming gemakkelijk intrekken en intrekkingen worden tijdig verwerkt.

Aan de slag

1. Hou in het verwerkingsregister bij voor welke verwerkingen toestemming moet worden gevraagd van betrokkenen.
2. Zorg ervoor dat bij verwerkingen waarvoor toestemming nodig is, de manier waarop toestemming wordt gevraagd en gegeven voldoet aan de eisen van de AVG. Dit betekent onder meer dat betrokkenen vooraf worden geïnformeerd over het doel waarvoor toestemming wordt gevraagd en dat de toestemming actief - geen opt-out maar opt-in - en vrijwillig wordt gegeven. Vraag bij kinderen jonger dan 16 jaar toestemming aan de ouders/verzorgenden.
3. Zorg ervoor dat de betrokkene toestemming altijd kan intrekken op een manier die net zo eenvoudig is als de manier waarop de toestemming is gegeven. Informeer de betrokkene vooraf over de mogelijkheid om de toestemming in te trekken.
4. Zorg ervoor dat achteraf aangetoond kan worden dat toestemming is gegeven, zowel digitaal als analoog.

Referentie naar andere normen en kaders

AVG Art. 4 sub 11
Art. 6 lid 1 sub a
Art. 7
Art. 8
Art. 9 lid 2 sub a
Art. 5 UAVG

Link naar relevante IB normen

RB.04 Geautomatiseerde besluitvorming en/of profilering

Norm

De organisatie voldoet aan de wettelijke vereisten voor geautomatiseerde individuele besluitvorming, waaronder profilering.

Waarom is dit nodig?

Mensen hebben volgens de AVG recht op een menselijke blik bij besluiten. Maak je als school gebruik van geautomatiseerde besluitvorming of profilering? Dan moet je dat doen volgens de regels van de AVG. Dat betekent onder andere dat je medewerkers en leerlingen goed informeert over het gebruik ervan en dat het mogelijk moet zijn om een nieuw besluit te nemen waarbij een mens de gegevens beoordeelt. Zo bescherm je medewerkers en leerlingen tegen onrechtmatige verwerking.

1 - Ad hoc

1 – Ad hoc

- a) Er is niet of onvoldoende bekend of er geautomatiseerde individuele besluitvorming en/of profilering binnen de organisatie plaatsvindt.

b) Betrokkenen worden niet of nauwelijks geïnformeerd over geautomatiseerde individuele besluitvorming en/of profilering

2 - Herhaalbaar

2 – Herhaalbaar

- a) Er is (enigszins) bekend dat de organisatie gebruik maakt van geautomatiseerde individuele besluitvorming en/of profilering, maar de organisatie heeft geen of beperkt begrip van de gebruikte algoritmes en/of er is geen of onvolledige documentatie hierover.
- b) DPIA's worden niet consequent voor elke nieuwe of gewijzigde geautomatiseerde individuele besluitvorming en/of profilering uitgevoerd.
- c) Betrokkenen worden op ad-hocbasis geïnformeerd over deze vorm van besluitvorming.
- d) Er zijn informele procedures voor het omgaan met geautomatiseerde besluitvorming en/of profilering, waaronder de mogelijkheid voor betrokkenen om hun standpunt kenbaar te maken en besluiten aan te vechten.

3 - Bepaald (streefniveau)

3 – Bepaald

- a) De organisatie heeft een volledig begrip van en documentatie, waaronder een algoritmeregister, over welke processen gebruik maken van (gedeeltelijke) geautomatiseerde individuele besluitvorming en/of profilering.
- b) Er zijn formele procedures geïmplementeerd voor geautomatiseerde besluitvorming en/of profilering, inclusief het informeren van betrokkenen en het bieden van mogelijkheden voor betrokkenen om hun standpunt kenbaar te maken en besluiten aan te vechten.
- c) Betrokkenen worden geïnformeerd over geautomatiseerde besluitvorming en/of profilering op een wijze die in overeenstemming is met de informatieplicht.
- d) Er wordt een DPIA uitgevoerd voor elke nieuwe geautomatiseerde besluitvorming en/of profilering.

4 - Beheerst

4 – Beheerst

- a) Geautomatiseerde besluiten en/of profilering, worden periodiek geëvalueerd. Periodiek worden gerelateerde DPIA's geëvalueerd. Daar waar nodig worden de privacywaarborgen verbeterd.
- b) De organisatie voert periodiek audits uit om te controleren of de processen van geautomatiseerde individuele besluitvorming en/of profilering voldoen aan de AVG-vereisten en andere wettelijke vereisten, zoals de AI Act.
- c) De organisatie communiceert proactief informatie over deze vorm van besluitvorming aan betrokkenen.

5 - Continu verbeteren

5 – Continu verbeteren

- a) Er is een (interne) tool waarmee geautomatiseerde besluiten en/of profilering eenvoudig kunnen worden bijgehouden en geëvalueerd op juistheid.
- b) De organisatie voorziet belanghebbenden van actuele informatie op basis waarvan automatische besluitvorming plaatsvindt.
- c) De organisatie past continu DPIA's toe op geautomatiseerde besluitvorming en/of profilering, waarbij de resultaten worden gebruikt om processen te verbeteren.

Aan de slag

1. Geef in het verwerkingsregister aan bij welke processen de organisatie gebruik maakt van geautomatiseerde besluitvorming en profilering.
2. Stel een procedure op voor het toepassen van geautomatiseerde besluitvorming en profilering. Neem hierin op hoe betrokkenen worden geïnformeerd en op welke manier zij in contact kunnen komen over het besluit met een echt (contact)persoon van de school, hun standpunt kenbaar kunnen maken of besluiten aan kunnen vechten die geautomatiseerd zijn genomen.

3. Informeer betrokkenen vooraf bij het toepassen van geautomatiseerde besluitvorming en profilering. En leg uit op basis van welke criteria of achterliggende gedachte het besluit tot stand komt.
4. Voer een DPIA uit voor elke nieuwe verwerking waarbij geautomatiseerde besluitvorming of profilering wordt toegepast.

Referentie naar andere normen en kaders

AVG Art. 13 lid 2 onder f
Art. 14 lid 2 onder g
Art. 22
Art. 40 UAVG

Link naar relevante IB normen

5. Samenwerking

Je school moet ervoor zorgen dat de samenwerking met andere organisaties en gegevensverstrekking aan derden tijdig wordt getoetst. Ook moet je de juiste privacyafspraken maken en passende waarborgen treffen om de privacy van betrokkenen te beschermen.

Wie is verantwoordelijk:

Eindverantwoordelijk: Schoolbestuur
Verantwoordelijk voor de uitvoering: Privacy Officer of IBP-adviseur, proceseigenaar
Geraadpleegd: Verwerker, FG
Geïnformeerd: FG

SW.01 AVG-rollen

Norm

De organisatie heeft de AVG-rol voor alle betrokken partijen die persoonsgegevens verwerken inzichtelijk en heeft conform de AVG met deze partijen afspraken gemaakt.

Waarom is dit nodig?

De school is verantwoordelijk voor alle gegevens die zij verwerkt of laat verwerken door andere partijen (leveranciers). Betrokkenen moeten erop kunnen vertrouwen dat jouw school goede afspraken heeft gemaakt met alle partijen waarmee ze samenwerkt, zodat er controle is op de verwerking van de gegevens. Met een helder vastgelegde rolverdeling kan de rechtmatige verwerking van persoonsgegevens worden beoordeeld, getoetst en gemonitord. Daarnaast stelt een goede rolverdeling de school in staat om de kwaliteit van processen te verbeteren.

1 - Ad hoc

1 – Ad hoc

- a) De organisatie heeft de AVG-rollen van de organisatie zelf en die van externe partijen die betrokken zijn bij verwerking van persoonsgegevens niet inzichtelijk gemaakt.
- b) Voorafgaand aan een verwerking voert de organisatie geen beoordeling uit om te bepalen of een externe optreedt als gegevensverwerker, gezamenlijke verwerkingsverantwoordelijke of zelfstandige verwerkingsverantwoordelijke.
- c) Er worden geen of nauwelijks afspraken gemaakt met verwerkers, gezamenlijke verwerkingsverantwoordelijken en eventueel zelfstandig verwerkingsverantwoordelijken.

2 - Herhaalbaar

2 – Herhaalbaar

- a) Medewerkers hebben beperkt bewustzijn van het belang van het onderscheiden van AVG-rollen.
- b) De organisatie heeft de AVG-rollen van de organisatie en die van externe partijen deels inzichtelijk gemaakt, maar dit is gefragmenteerd en inconsistent.
- c) Er wordt incidenteel een beoordeling uitgevoerd om te bepalen of de externe partij optreedt als gegevensverwerker, gezamenlijke verwerkingsverantwoordelijke, of zelfstandige verwerkingsverantwoordelijke, maar dit gebeurt niet systematisch en is sterk afhankelijk van individuen of afdelingen.
- d) Er worden in sommige gevallen afspraken gemaakt met verwerkers, gezamenlijke verwerkingsverantwoordelijken en eventueel zelfstandig verwerkingsverantwoordelijken, maar dit is niet uniform.
- e) Indien gebruik wordt gemaakt van externe verwerkers, is er geen of onvoldoende inzicht in subverwerkers en/of in de afspraken met de subverwerkers.

3 - Bepaald (streefniveau)

3 – Bepaald

- a) De organisatie heeft de AVG-rollen van de organisatie en die van externe partijen duidelijk en inzichtelijk gemaakt en medewerkers zijn zich bewust van het belang om AVG-rollen te onderscheiden.
- b) Er is een gestandaardiseerd proces om voorafgaand aan elke gegevensverwerking te beoordelen en vast te stellen of de externe partij optreedt als gegevensverwerker, gezamenlijke verwerkingsverantwoordelijke of zelfstandige verwerkingsverantwoordelijke.
- c) Er worden consistent afspraken gemaakt met verwerkers, gezamenlijke verwerkingsverantwoordelijken en eventueel zelfstandig verwerkingsverantwoordelijken. De overeenkomsten bevatten de elementen die in de AVG, artikel 28 lid 3 zijn voorgeschreven en afspraken hoe wijzigingen (bijvoorbeeld wijziging van subverwerkers) worden gemeld.
- d) Het beheer van overeenkomsten met verwerkers, zelfstandig verwerkingsverantwoordelijken en gezamenlijke verwerkingsverantwoordelijken is adequaat belegd binnen de organisatie.

4 - Beheerst

4 – Beheerst

- a) AVG-rollen van externe partijen worden periodiek geëvalueerd. Indien noodzakelijk worden beleid en procedures aangepast.
- b) Naleving van de afspraken die zijn gemaakt met verwerkers en gezamenlijke verwerkingsverantwoordelijken wordt periodiek getoetst of geaudit.
- c) De afspraken met verwerkers, gezamenlijke verwerkingsverantwoordelijken en eventueel zelfstandig verwerkingsverantwoordelijken worden periodiek geëvalueerd en aangepast indien nodig.
- d) Het beheer en evaluatie van overeenkomsten met verwerkers, zelfstandig verwerkingsverantwoordelijken en gezamenlijke verwerkingsverantwoordelijken is goed georganiseerd en wordt periodiek geëvalueerd en waar nodig aangepast.
- e) Training en bewustwording over AVG-rollen zijn geïntegreerd in de processen en procedures van de organisatie.

5 - Continu verbeteren

5 – Continu verbeteren

- a) Er is een eenvoudig en toegankelijk tool/systeem dat een overzicht/rapportages biedt van de AVG-rollen van externe partijen.
- b) De organisatie is in staat om snel en effectief te reageren op veranderingen in AVG-rollen van externe partijen, en past procedures en overeenkomsten dienovereenkomstig aan.

Aan de slag

1. Zorg ervoor dat de rollen van partijen die persoonsgegevens verwerken duidelijk zijn vastgelegd en beschreven.

2. Stel een procedure vast waarmee vooraf wordt beoordeeld of een partij waaraan gegevens worden verstrekt verwerker of (gezamenlijk) verwerkingsverantwoordelijke is.
3. Maak medewerkers bewust van de verschillende rollen en het belang van het onderscheid daarvan.
4. Maak afspraken met verwerkers, gezamenlijke verwerkingsverantwoordelijken en eventueel zelfstandig verwerkingsverantwoordelijken. Zorg ervoor dat deze afspraken voldoen aan de eisen die hiervoor gelden op grond van de AVG.
5. Beleg het beheer van de afspraken goed binnen de organisatie.

Referentie naar andere normen en kaders

AVG Art.26, Art.28

Link naar relevante IB normen

SC.03

SW.02 Toetsing gegevensverstrekking aan derden

Norm

De organisatie toetst ieder voornemen om persoonsgegevens aan een derde partij te verstrekken aan de relevante wet- en regelgeving.

Waarom is dit nodig?

Door de gegevensverstrekking vooraf te toetsen aan relevante wet- en regelgeving, zorg je ervoor dat alleen die persoonsgegevens worden verwerkt die relevant zijn, overeenkomstig het vooraf vastgestelde doel en gebaseerd op de juiste grondslag. Als je dit procesmatig inregelt, vergroot je de validiteit en de kwaliteit van de gegevensuitwisseling.

1 - Ad hoc

1 – Ad hoc

- a) De organisatie heeft geen eenduidige, gestandaardiseerde procedure vastgesteld voor de toetsing van gegevensverstrekking aan derden.
- b) Het delen van persoonsgegevens met externe partijen gebeurt zonder voorafgaande toetsing of er is weinig tot geen bewustzijn van het belang van deze toetsing.

2 - Herhaalbaar

2 – Herhaalbaar

- a) De organisatie voert sporadisch en ongestructureerd toetsingen uit op voorgenomen gegevensverstrekking aan externe partijen, zonder een systematische benadering en in overeenstemming met de toepasselijke (privacy)wetgeving.
- b) Een coherente, organisatiebrede procedure ontbreekt, wat leidt tot inconsistenties en variatie in de kwaliteit van de toetsingen.
- c) Medewerkers en/of afdelingen zoals inkoop, management en control of onderzoekers, hebben beperkt bewustzijn van het belang van het toetsen van de gegevensverstrekking aan externe partijen.

3 - Bepaald (streefniveau)

3 – Bepaald

- a) De organisatie heeft een uniform, organisatiebreed kader geïmplementeerd voor het toetsen van gegevens-

verstrekking aan externe partijen, dat consequent wordt toegepast in de gehele organisatie.

b) De organisatie heeft het kader met daarin zowel het toetsingsproces als de besluitvorming daaromtrent gedocumenteerd.

c) Alle medewerkers zijn goed geïnformeerd over het belang van voorafgaande toetsing van de gegevensverstrekking aan externe partijen en zijn actief betrokken bij deze processen.

d) Medewerkers weten wie ze kunnen benaderen om te toetsen of een eenmalige gegevensverstrekking in overeenstemming is met de wet- en regelgeving.

4 - Beheerst

4 – Beheerst

a) De organisatie voert periodiek systematische controles uit om ervoor te zorgen dat de gegevensverstrekking aan externe partijen steeds voldoet aan de meest recente wet- en regelgeving.

b) De toetsingsprocedures worden periodiek geëvalueerd en indien nodig aangepast.

c) Training en bewustmaking over gegevensverstrekking aan externe partijen zijn geïntegreerd in de reguliere bedrijfsprocessen en -procedures.

d) Er is een gemakkelijk vindbaar overzicht van alle gegevensverstrekkingen aan externe partijen beschikbaar, bijvoorbeeld via een specifieke interne tool of systeem.

5 - Continu verbeteren

5 – Continu verbeteren

a) De organisatie is in staat om snel te reageren op wijzigingen in wet- en regelgeving die de gegevensverstrekking aan externe partijen kunnen beïnvloeden, en ze kan procedures en praktijken dienovereenkomstig aanpassen.

Aan de slag

1. Stel een kader vast waarmee het verstrekken van persoonsgegevens aan externe partijen kan worden getoetst.
2. Zorg ervoor dat dit kader bekend is en consequent wordt toegepast binnen de hele schoolorganisatie.
3. Zorg ervoor dat bij medewerkers bekend is bij wie ze terecht kunnen om te beoordelen of een (eenmalige) verstrekking van persoonsgegevens is toegestaan.
4. Documenteer besluiten die worden genomen over het verstrekken van persoonsgegevens aan externe partijen.

Referentie naar andere normen en kaders

AVG Art.5, Art.6

Link naar relevante IB normen

SC.03, DM.05

SW.03 Doorgifte buiten de EER

Norm

Doorgifte van persoonsgegevens buiten de EER vindt uitsluitend plaats wanneer een passend beschermingsniveau is gewaarborgd.

Waarom is dit nodig?

Bij gegevensverwerking buiten de Europese Economische Ruimte (EER) moeten er (juridische, technische en organisatorische) waarborgen zijn dat het beschermingsniveau voldoet aan de AVG, zodat de persoonsgegevens

veilig en voldoende beschermd blijven. Betrokkenen moeten hun privacyrechten kunnen blijven uitoefenen zoals verwoord in het privacybeleid en privacyreglement. Een goed proces waarbij verwerkingen vooraf getoetst worden op rechtmatigheid draagt bij aan de juiste bescherming van persoonsgegevens.

1 - Ad hoc

1 – Ad hoc

- a) Binnen de organisatie is er onvoldoende bekendheid over de procedures die moeten worden gevolgd bij het overdragen van gegevens buiten de EER.
- b) De organisatie heeft geen (duidelijk) inzicht in de landen waaraan persoonsgegevens worden doorgegeven.
- c) Periodieke toetsing van de naleving van wet- en regelgeving met betrekking tot de doorgifte van persoonsgegevens aan derde landen (buiten de EER) ontbreekt.

2 - Herhaalbaar

2 – Herhaalbaar

- a) De organisatie voert voorafgaand aan een voorgenomen doorgifte naar een derde land buiten de EER een toetsing uit of bij doorgifte de verwerking aan een passend beschermingsniveau voldoet, maar het proces is niet (volledig) gedocumenteerd en de kennis en expertise is slechts bij een beperkt aantal individuen binnen de organisatie aanwezig.
- b) Er is geen gestandaardiseerde procedure voor het documenteren van landen waaraan persoonsgegevens worden doorgegeven, wat het risico op inconsistenties en fouten verhoogt.

3 - Bepaald (streefniveau)

3 – Bepaald

- a) De organisatie voert voorafgaand aan een voorgenomen doorgifte buiten de EER een systematische toetsing uit om te beoordelen of bij doorgifte de verwerking aan een passend beschermingsniveau voldoet.
- b) Er is een duidelijk en consistent proces voor het documenteren van landen waaraan persoonsgegevens worden doorgegeven.
- c) Periodiek wordt getoetst of de doorgifte naar derde landen buiten de EER (nog) aan de wet- en regelgeving voldoet. Het proces voor deze toetsing is gedocumenteerd en bekend bij de medewerkers.

4 - Beheerst

4 – Beheerst

- a) De organisatie evalueert periodiek de doorgiftes buiten de EER en past indien nodig de (toets)processen aan.
- b) De periodieke evaluaties worden ondersteund door bewustwordingscampagnes en/of training om kennis en bewustzijn over doorgiftes buiten de EER binnen de organisatie te verhogen.

5 - Continu verbeteren

5 – Continu verbeteren

- a) De organisatie heeft een tool geïmplementeerd om inzicht te krijgen in gegevensverstrekkingen, waaronder doorgiftes naar derde landen, wat ook het proces van het monitoren en periodiek evalueren van de gegevensverstrekkingen vergemakkelijkt.
- b) De organisatie is in staat om te reageren op veranderingen in de omstandigheden of wet- en regelgeving over doorgifte buiten de EER.

Aan de slag

1. Beoordeel bij het doorgeven van persoonsgegevens aan landen buiten de EER vooraf of er een passend beschermingsniveau is en documenteer deze beoordeling.

2. Houd een overzicht bij van de landen waaraan persoonsgegevens worden doorgegeven en van de verwerkingen waarbij dit buiten de EER gebeurt. Leg dit bijvoorbeeld vast in het verwerkingsregister.
3. Toets aan de hand van een vastgestelde procedure ten minste één keer per jaar of de doorgifte van persoonsgegevens aan landen buiten de EER nog voldoet aan de wet- en regelgeving. Documenteer de uitkomsten van de toetsing.
4. Houd internationale ontwikkelingen, besluiten en afspraken van de Europese Commissie en uitspraken van het Europese Hof van Justitie over het doorgeven van persoonsgegevens goed in de gaten. Denk bijvoorbeeld aan het Data Privacy Framework.

Referentie naar andere normen en kaders

AVG Art.27, Art.44, Art.45, Art.46, Art.47, Art.48, Art.49

Link naar relevante IB normen

6. Beveiliging

Informatiebeveiliging en privacy (IBP) zijn onlosmakelijk met elkaar verbonden. Zonder de juiste beveiligingsmaatregelen kan je school de privacy van leerlingen en medewerkers niet beschermen. In het funderend onderwijs gebruiken scholen het deel Informatiebeveiliging van dit Normenkader om de juiste beveiligingsmaatregelen te nemen. Daarnaast moet je school een proces hebben om beveiligingsincidenten en datalekken tijdig (intern) te melden en zo nodig te melden als datalek bij de Autoriteit Persoonsgegevens.

Wie is verantwoordelijk:

Eindverantwoordelijk: Schoolbestuur

Verantwoordelijk voor uitvoering: Privacy Officer of IBP-adviseur, it-verantwoordelijke

Geraadpleegd: Verwerker of it-leverancier, FG

Geïnformeerd: (G)MR, Raad van Toezicht, indien relevant AP bij datalek

GB.01 Datalekken detectie, classificatie en afhandeling

Norm

De organisatie heeft een proces vastgesteld en gedocumenteerd voor de detectie, classificatie en afhandeling van datalekken.

Waarom is dit nodig?

Scholen verwerken veel (gevoelige) gegevens. Een datalek kan aanzienlijke en ongewenste gevolgen hebben voor betrokkenen en moet daarom tijdig en adequaat worden aangepakt. Een heldere en effectieve procedure is cruciaal voor een efficiënte en snelle afhandeling van datalekken. Dit minimaliseert de impact voor betrokkenen als leerlingen en medewerkers én voor jouw school. Het stelt daarnaast betrokkenen in staat om tijdig de nodige maatregelen te treffen. Door (beveiligings)incidenten en (potentiële) datalekken te registreren en structureel te evalueren, verminder je de kans op herhaling. Bovendien vergroot dit de bewustwording rond informatiebeveiliging en privacy.

1 - Ad hoc

1 – Ad hoc

- a) Er ontbreekt een (centraal) meldpunt voor (beveiligings)incidenten en (potentiële) datalekken dat toegankelijk is voor alle medewerkers, leerlingen en overige betrokkenen.
- b) Er is geen gestructureerd proces voor het detecteren, classificeren en afhandelen van datalekken.
- c) Er is niet duidelijk wanneer een (beveiligings)incident een datalek is.

- d) Incidenten worden afgehandeld op ad-hocbasis en worden niet geëvalueerd.
- e) Er is geen datalekkenregister.

2 - Herhaalbaar

2 – Herhaalbaar

- a) Er is geen makkelijk vindbaar meldpunt voor (beveiligings)incidenten en (potentiële) datalekken voor alle medewerkers, leerlingen en overige betrokkenen, en/of het is niet gemakkelijk toegankelijk.
- b) Er is een informeel proces voor het detecteren, classificeren en afhandelen van datalekken, maar medewerkers zijn onvoldoende opgeleid om adequaat te reageren op incidenten waarbij persoonsgegevens zijn betrokken.
- c) Classificatie van incidenten waarbij persoonsgegevens zijn betrokken op impact/risico voor betrokkenen is afhankelijk van de individuele medewerker die de classificatie uitvoert.
- d) Evaluatie van incidenten waarbij persoonsgegevens zijn betrokken wordt ad hoc uitgevoerd.
- e) Het datalekkenregister wordt ad hoc ingevuld.

3 - Bepaald (streefniveau)

3 – Bepaald

- a) Er is een makkelijk vindbaar en gemakkelijk toegankelijk meldpunt voor (beveiligings)incidenten en (potentiële) datalekken.
- b) Er is een gedetailleerd proces gedefinieerd en gedocumenteerd voor het detecteren, classificeren en afhandelen van datalekken. Het proces omvat ten minste:
 - een beschrijving van rollen, verantwoordelijkheden en contactpersonen
 - detectie en identificatie van een datalek
 - een risicobeoordeling/afwegingskader waar het al dan niet melden van een datalek onderdeel van is
 - respons- en escalatie
 - beheersing
 - herstel
 - evaluatie.
- c) Incidenten worden systematisch geëvalueerd om verbeteringen te identificeren.
- d) De resultaten van de evaluaties worden met het management gedeeld.

4 - Beheerst

4 – Beheerst

- a) Het proces voor het detecteren, classificeren en afhandelen van datalekken wordt periodiek geëvalueerd om de effectiviteit ervan te waarborgen en indien nodig aangepast.
- b) De vindbaarheid van het privacy meldpunt wordt periodiek geëvalueerd.

5 - Continu verbeteren

5 – Continu verbeteren

- a) Het proces voor het detecteren, classificeren en afhandelen van datalekken is volledig geïntegreerd en er is een proactieve aanpak om mogelijke toekomstige incidenten te identificeren en te voorkomen.
- b) Verbeteringen die voortvloeien uit de evaluatie van datalekken worden snel en consequent geïmplementeerd.
- c) De resultaten van de evaluatie van datalekken worden gedeeld met het management en indien van toepassing binnen de gehele organisatie.
- d) Onderzoek of een opgetreden datalek ook bij andere verwerkingen kan optreden is onderdeel van evaluaties.

Aan de slag

1. Zorg voor een goed toegankelijk meldpunt voor beveiligingsincidenten en - potentiële - datalekken dat ook buiten schooltijden bereikbaar is. Zorg ervoor dat alle medewerkers en verwerkers bekend zijn met dit meldpunt.

2. Stel een procedure op voor de detectie, beoordeling en afhandeling van datalekken.
3. Pas de datalekkenprocedure consistent toe bij ieder beveiligingsincident.
4. Documenteer ieder beveiligingsincident en datalek. Neem van ieder incident ten minste op: de feiten over het incident, de gevolgen ervan en de genomen maatregelen.
5. Evalueer ieder incident en deel de resultaten van de evaluatie met de schoolleider en het schoolbestuur.

Referentie naar andere normen en kaders

AVG Art.2 sub 12, Art.33, Art.34

Link naar relevante IB normen

IM.01, IM.02, IM.03

GB.02 Melding datalekken

Norm

De organisatie heeft een gestructureerd proces ingericht en gedocumenteerd voor het tijdig en volledig melden van datalekken aan de relevante partijen, inclusief de Autoriteit Persoonsgegevens (AP) en de betrokkenen.

Waarom is dit nodig?

Wanneer je wordt geïnformeerd over een beveiligingsincident in je school, is het essentieel dat je dit zo snel mogelijk beoordeelt. Hierdoor ben je in staat om (potentiële) datalekken binnen de wettelijke termijn te melden bij de AP en de betrokkenen te informeren, zodat die eventueel maatregelen kunnen treffen. Door vooraf een proces in te richten, zorg je ervoor dat incidenten en datalekken op een juiste manier worden afgehandeld en geëvalueerd. Zo voorkom je herhaling.

1 - Ad hoc

1 – Ad hoc

- a) Er is geen proces voor melden van datalekken aan de AP en betrokkenen.
- b) Er is geen duidelijkheid over wie verantwoordelijk is voor het melden van een datalek aan de AP en betrokkenen.
- c) Er zijn geen vastgestelde tijdslijnen voor het melden van een datalek aan de AP en betrokkenen.
- d) Er is geen woordvoerder voor de communicatie over (mogelijke) datalekken met betrokkenen en/of media.

2 - Herhaalbaar

2 – Herhaalbaar

- a) Er bestaat een Informeel proces voor het melden van datalekken aan de AP en betrokkenen, maar de implementatie en naleving zijn inconsistent.
- b) Verantwoordelijkheden voor het afhandelen en communiceren van datalekken zijn gedefinieerd, maar zijn niet altijd duidelijk voor alle betrokken partijen.
- c) De tijdslijnen waarbinnen datalekken worden gemeld zijn wisselend en er is geen vastgesteld proces voor het documenteren van de afhandeling van een datalek. Classificatie van de ernst (risicobeoordeling) van een datalek is afhankelijk van de betrokkenen.

3 - Bepaald (streefniveau)

3 – Bepaald

- a) Er is een gedetailleerd en gedocumenteerd proces voor het melden van datalekken aan de AP en betrokkenen, met daarin ten minste:

- Conceptberichten voor communicatie (onder anderen voor betrokkenen)
 - Duidelijk gedefinieerde verantwoordelijkheden
 - Documentatievereisten en tijdslijnen
- c) Er is een crisiscommunicatieplan voor datalekken met hoge impact.
- d) Het proces wordt consistent nageleefd.

4 - Beheerst

4 – Beheerst

- a) Het proces voor het melden van datalekken aan de AP en betrokkenen is volledig geïntegreerd in de organisatie, met consistente uitvoering en naleving.
- b) Het proces voor het melden van datalekken aan de AP en betrokkenen wordt periodiek geëvalueerd en, indien nodig, aangepast.
- c) Het crisiscommunicatieplan voor datalekken met hoge impact wordt periodiek geoefend, en indien nodig herzien.

5 - Continu verbeteren

5 – Continu verbeteren

- a) Het proces voor het melden van datalekken aan de AP en betrokkenen is een standaard onderdeel van de bedrijfsvoering, wordt systematisch nageleefd en continu geëvalueerd en verbeterd.
- b) Het management wordt systematisch geïnformeerd over alle datalekken en genomen maatregelen.
- c) Er bestaat een hiërarchie (escalatieregels) voor escalatie naar de juiste managementniveaus.

Aan de slag

1. Stel een proces op voor het melden van datalekken aan de Autoriteit Persoonsgegevens en aan betrokkenen. Leg hierin vast welke informatie er nodig is om een volledige melding te kunnen doen en binnen welke termijn dit moet gebeuren en door wie.
2. Meld datalekken tijdig bij de Autoriteit Persoonsgegevens en bij betrokkenen. Meld datalekken waarvan nog niet alle benodigde informatie bekend is als voorlopig bij de Autoriteit Persoonsgegevens. Deze voorlopige melding kan later worden aangevuld, aangepast of ingetrokken.
3. Stel conceptberichten op voor de melding van datalekken aan betrokkenen.
4. Stel een crisiscommunicatieplan op voor datalekken met veel impact.

Referentie naar andere normen en kaders

AVG Art.4 sub 12, Art.33, Art.34

Link naar relevante IB normen

IM.01, IM.02, IM.03

GB.03 Beveiliging persoonsgegevens

Norm

De organisatie neemt passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen. Om te zorgen voor een passend beveiligingsniveau voldoet de organisatie aan de informatiebeveiligingsnormen van het Normenkader IBP.

Waarom is dit nodig?

Iedere leerling en medewerker moet kunnen leren en werken in een digitaal veilige omgeving. Daarom moet je als school passende technische en organisatorische maatregelen nemen om persoonsgegevens te beschermen tegen bijvoorbeeld verlies, wijziging, vernietiging, of ongeoorloofde toegang of verstrekking. Door te voldoen aan de normen van het deel informatiebeveiliging zorg je ervoor dat persoonsgegevens op de juiste manier beveiligd zijn.

1 - Ad hoc

nvt

2 - Herhaalbaar

nvt

3 - Bepaald (streefniveau)

nvt

4 - Beheerst

nvt

5 - Continu verbeteren

nvt

Aan de slag

1. Implementeer de informatiebeveiligingsnormen van het Normenkader IBP en evalueer de toepassing en implementatie daarvan op terugkerende basis
2. Houd bij het nemen van beveiligingsmaatregelen voor persoonsgegevens specifiek rekening met de risico's voor de rechten en vrijheden van betrokkenen, en niet alleen met risico's voor de organisatie.

Referentie naar andere normen en kaders

AVG Art.32

Link naar relevante IB normen

Gehele Normenkader IBP - deel IB

7. Verantwoording

Je school evalueert de naleving van de AVG en rapporteert hierover onder andere in het jaarverslag.

Wie is verantwoordelijk:

Eindverantwoordelijk: Schoolbestuur

Verantwoordelijk voor uitvoering: Schoolbestuur, bestuurssecretaris

Geraadpleegd: FG

Geïnformeerd: Raad van Toezicht, (G)MR

VW.01 Rapportage naleving AVG

Norm

De organisatie houdt periodiek interne en externe stakeholders op de hoogte over de naleving van de AVG.

Waarom is dit nodig?

Met een duidelijke, toegankelijke en regelmatige rapportage aan in- en externe belanghebbenden over de wijze waarop de school zorgt voor een zorgvuldige verwerking en adequate beveiliging van persoonsgegevens, legt het schoolbestuur verantwoording af over naleving van de AVG. Zo kunnen betrokkenen als leerlingen en medewerkers vertrouwen op een goede naleving van de AVG binnen je school. Schoolbesturen zijn verplicht om vanaf schooljaar 2023-2024 in hun jaarverslag aandacht te besteden aan informatiebeveiliging en privacy.

1 - Ad hoc

1 – Ad hoc

- a) Er wordt geen periodiek verslag gemaakt om interne (inclusief het schoolbestuur) en externe stakeholders te informeren over de omgang met en bescherming van persoonsgegevens binnen de organisatie.
- b) Informatie van afdelingen over de omgang met en bescherming van persoonsgegevens binnen hun afdeling of hun processen wordt niet periodiek (centraal) verzameld. Hierdoor kan er geen organisatiebreed inzicht worden verschaft over de naleving van de AVG

2 - Herhaalbaar

2 – Herhaalbaar

- a) Er wordt periodiek een verslag opgesteld voor zowel interne (inclusief het schoolbestuur) als externe stakeholders over de omgang met en bescherming van persoonsgegevens binnen de organisatie, maar dit proces is niet gedocumenteerd en de FG wordt niet consequent betrokken.
- b) Informatie van afdelingen over de omgang met en bescherming van persoonsgegevens wordt periodiek (centraal) verzameld, maar dit proces is niet volledig gedocumenteerd en gebeurt niet op een structurele en georganiseerde manier.

3 - Bepaald (streefniveau)

3 – Bepaald

- a) Er wordt een gestructureerd en gedocumenteerd proces gevolgd voor het opstellen van een periodiek verslag waarin zowel interne (inclusief het schoolbestuur) als externe stakeholders worden geïnformeerd over de omgang met en bescherming van persoonsgegevens binnen de organisatie. De FG wordt betrokken en geraadpleegd bij het opstellen van dit verslag.
- b) Informatie van afdelingen over de omgang met en bescherming van persoonsgegevens wordt periodiek centraal verzameld op een gestructureerde manier, waardoor de bestuursorganen organisatiebreed inzicht kunnen krijgen in de naleving van de AVG.
- c) Dit proces omvat het periodiek opstellen van een organisatieverslag waarin verschillende aspecten worden behandeld, bijvoorbeeld het globale overzicht van het verwerkingsregister, uitgevoerde DPIA's, verslag over datalekken, verzoeken rechten van betrokkenen, (evt. resultaten van een privacy benchmark), klachten, en verbeterplannen.
- d) De verantwoordelijkheden voor het opstellen en verspreiden van dit verslag zijn duidelijk aantoonbaar toegewezen.

4 - Beheerst

4 – Beheerst

- a) De inhoudelijke elementen van de rapportage en het rapportageproces worden periodiek geëvalueerd en indien nodig aangepast.
- b) Op basis van rapportage worden verbeterplannen opgesteld en wordt gerapporteerd over de uitvoering hiervan.

5 - Continu verbeteren

5 – Continu verbeteren

- a) Er is een volledig geïntegreerd proces voor het opstellen van periodieke rapportages en het centraal verzamelen van informatie van afdelingen. Dit proces wordt systematisch nageleefd en continu geëvalueerd en verbeterd.
- b) Naast de reguliere periodieke rapportage, worden interne en externe stakeholders ook ad hoc geïnformeerd over belangrijke in- en externe ontwikkelingen met betrekking tot de bescherming van persoonsgegevens.
- c) Er wordt gebruik gemaakt van tools en methodes om informatie op een toegankelijke en begrijpelijke manier te presenteren, bijvoorbeeld via infographics of animaties.
- d) Er vindt periodiek uitwisseling plaats met andere organisatie om ervaringen, best practices en leerpunten te delen op het gebied van AVG-naleving en transparantie, verantwoording en rapportage.

Aan de slag

1. Stel een periodiek verslag op waarin zowel het schoolbestuur als de Raad van Toezicht en (G)MR worden geïnformeerd over de omgang met en bescherming van persoonsgegevens binnen de organisatie. Betrek de FG bij het opstellen van dit verslag. Neem het verslag over de naleving van de AVG op in het (jaarlijkse) organisatieverslag. Verwerk hierin informatie over het verwerkingsregister, uitgevoerde DPIA's, datalekken, verzoeken van uitoefening van rechten van betrokkenen, resultaten van de privacy self assessment en verbeterplannen.
2. Verzamel informatie van scholen over de omgang met en bescherming van persoonsgegevens periodiek en op een gestructureerde manier, zodat het schoolbestuur organisatiebreed inzicht krijgt over de naleving van de AVG.

Referentie naar andere normen en kaders

AVG Art.5 lid 2, Art.39

Link naar relevante IB normen