INFORMATIEBEVEILIGINGS- EN PRIVACY BELEID ELEVANTIO (IBP)

Juni 2022

Inhoud

1 HET BELANG VAN INFORMATIEBEVEILIGING EN PRIVACY 3
2 TOELICHTING INFORMATIEBEVEILIGING EN PRIVACY 3

2.1 TOELICHTING INFORMATIEBEVEILIGING 3
2.2 TOELICHTING PRIVACY 3
2.3 VERVLECHTING INFORMATIEBEVEILIGING EN PRIVACY 3

3 DOEL EN REIKWIJDTE 4

3.1 DOEL 4
3.2 REIKWIJDTE 4

4 BELEID – HOE DOEN WE DAT? 5
5 UITWERKING VAN HET BELEID – WAT DOEN WE? 6

5.1 RELEVANTE WET- EN REGELGEVING 6
5.2 BASISREGELS BIJ HET OMGAAN MET PERSOONSGEGEVENS 7
5.3 ONDERSTEUNENDE RICHTLIJNEN EN PROCEDURES 7
5.4 VOORLICHTING EN BEWUSTZIJN 7
5.5 CLASSIFICATIE EN RISICOANALYSE 8
5.6 INCIDENTEN EN DATALEKKEN 8
5.7 PLANNING EN CONTROLE 8
5.8 NALEVING EN SANCTIES 8
5.9 LOGGING EN MONITORING 9

6 ORGANISATIE - WIE DOET WAT? 9

6.1 ROLLEN EN VERANTWOORDELIJKHEDEN 9

BIJLAGE 1: ONDERSTEUNENDE RICHTLIJNEN EN PROCEDURES 11
BIJLAGE 2: ORGANISATIE; WIE DOET WAT 12
BIJLAGE 3: REGELING TAKEN EN BEVOEGDHEDEN FUNCTIONARIS GEGEVENSBESCHERMING 15
BIJLAGE 4: BEGRIPPENLIJST 18

1 Het belang van informatiebeveiliging en privacy

Het onderwijs is in toenemende mate afhankelijk van informatie en ict. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ict. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ict en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van **informatiebeveiliging en privacy** (afgekort tot IBP) in een IBP-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

2 Toelichting informatiebeveiliging en privacy

2.1 Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden.
Informatiebeveiliging richt zich op de volgende aspecten:

- Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- Integriteit: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot ongewenste risico's in het onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

2.2 Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerking:
Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

2.3 Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom

samengevoegd tot één proces: IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis op informatiebeveiliging en privacy binnen Elevantio te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

3 Doel en reikwijdte

3.1 Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan Elevantio persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het informatiebeveiligings- en privacy beleid (IBP-beleid) is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene (o.a. medewerkers, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en Elevantio voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

- Het IBP-beleid binnen Elevantio geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers, vrijwilligers, stagiaires en externe relaties (inhuur / outsourcing). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.

- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Elevantio waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen, zoals sollicitanten, vrijwilligers en stagiaires waarvan Elevantio persoonsgegevens verwerkt.

- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Elevantio Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de school kan worden aangesproken. (b.v. uitspraken van medewerkers, vrijwilligers, stagiaires en leerlingen in discussies, op (persoonlijke pagina's van) websites en of social media.)

- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van Elevantio evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het IBP-beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

- IBP-beleid heeft binnen Elevantio raakvlakken met:

- *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen
- *Personeels- en organisatiebeleid;* met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties
- *IT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ict en (digitale) leermiddelen
- *Medezeggenschap* van leerlingen, hun ouders/verzorgers en medewerkers

4 Beleid – Hoe doen we dat?

Elevantio hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het schoolbestuur van Elevantio neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.

2. Elevantio voldoet aan alle relevante wet- en regelgeving.

3. Bij Elevantio is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van Elevantio om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen te allen tijde hun toestemming herzien.

4. Elevantio zal alle betrokkenen helder en actief informeren over de verwerkingen van de hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering.

5. Elevantio legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Elevantio voldoet hiermee aan de documentatieplicht.

6. Binnen Elevantio is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten. (hierbij valt o.a. te denken aan het opstellen van wachtwoordbeleid, toegangsbeleid, clear desk policy enz.)

7. Elevantio is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.

8. Elevantio classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.

9. Elevantio sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.

10. Elevantio verwacht van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Elevantio heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

11. Informatiebeveiliging en privacy is bij Elevantio een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

12. Elevantio kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vóóraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.

13. Elevantio neemt passende technische (beveiligings-)maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren.
    Aangezien de infrastructuur deels elders wordt beheerd en/of gegevens elders worden verwerkt legt Elevantio aanvullende afspraken vast over de technische maatregelen.

14. Elevantio zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen

5 Uitwerking van het beleid – Wat doen we?

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten en is daarmee de minimale invulling van het beleid.

5.1 Relevante wet- en regelgeving

De uitwerking van het beleid voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs
- Wet goed onderwijs en goed bestuur PO
- Wet onderwijstoezicht
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beveiligingsmaatregelen.

De bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy' zijn leidend bij het maken van afspraken met leveranciers, die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken.

5.2 Basisregels bij het omgaan met persoonsgegevens

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake verwerking persoonsgegevens (art.5 AVG) leidend. Deze zijn samengevat in de **vijf vuistregels** met betrekking tot de omgang met persoonsgegevens te weten:

1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.

2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen.

3. **Dataminimalisatie**: bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding tot het doel (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (subsidiar). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.

4. **Transparantie**: de school legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Tevens kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.

5. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

5.3 Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Bijlage 1 geeft een overzicht van de diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

5.4 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hier een belangrijke factor. Daarom wordt het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, leerlingen en gasten. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de teamleider BMO (verantwoordelijke IBP), de FG, en de werkgroep AVG met het bestuur als eindverantwoordelijke.

5.5 Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de betrouwbaarheidsaspecten die van belang zijn.
Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden. Vanaf de start van nieuwe (ict)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

5.6 Incidenten en datalekken

Alle medewerkers, die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister. Alle (beveiligings)incidenten kunnen worden gemeld doormiddel van het sturen van een mail naar privacy@elevantio.nl.
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

5.7 Planning en controle

Dit IBP-beleid wordt minimaal elke twee jaar getoetst en bijgesteld door het bestuur. Hierbij wordt rekening gehouden met:

- De status van de informatiebeveiliging als geheel (beleid, organisatie, risico's);
- de actuele geinventariseerde risico's;
- de effectiviteit van de genomen maatregelen en aantoonbare werking daarvan

Daarnaast kent Elevantio een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen.

5.8 Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, etcetera.
Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de het bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het bestuur vast te stellen reglement (bijlage 3: regeling taken en bevoegdheden Functionaris Gegevensbescherming).

Mocht de naleving van dit beleid ernstig tekortschieten, dan kan Elevantio de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

5.9 Logging en monitoring

Logging en monitoring door de IT-afdeling zorgt ervoor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in- uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk.

6 Organisatie - Wie doet wat?

6.1 Rollen en verantwoordelijkheden

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol.

Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen bij Elevantio.

Richtinggevend	**Eindverantwoordelijk**	
	College van Bestuur	• *Eindverantwoordelijk* • *IBP-beleidsvorming, -vastlegging en communiceren ervan* • *Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens* • *Organisatie IBP inrichten; toewijzen van de taken en rollen* • *Evalueren toepassing en werking IBP-beleid op basis van rapportages*
Sturend	**Uitwerken beleid / inhoudelijk verantwoordelijk**	
	Teamleider BMO	• *Voorbereiden opstellen IBP-beleid, Classificatie/risicoanalyse* • *Inhoudelijk verantwoordelijk voor uitwerking van het IBP-beleid* • *Adviseert verwerkingsverantwoordelijke (CvB) over IBP* • *Uitwerken algemeen IBP-beleid naar specifiek beleid op een uniforme manier* • *Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering van het IBP-beleid te ondersteunen* • *Evalueren van het IBP-beleid en de maatregelen*
	Functionaris voor gegevensbescherming	• *Toezicht houden op naleving privacy wetgeving* • *Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens* • *Voorlichting privacy geven en stimuleren van bewustwording* • *Afwikkeling IBP klachten en incidenten*

	Domeinverantwoordelijke/proceseigenaar: Directeuren en Teamleiders Financiën, Facilitair, HRM en Onderwijs / BICT	• *Risicoanalyse in samenwerking met teamleider BMO* • *Toegangsbeleid zowel fysieke toegang als digitale toegang vaststellen en laten goedkeuren door de verwerkingsverantwoordelijke* • *Regelmatig de (netwerk)toegangsrechten van gebruikers beoordelen, controleren en vastleggen*
Uitvoerend	**Uitvoeren beleid / naleven beleid**	
	Werkgroep AVG BICT/ ICT-beheerder (intern en extern) Alle medewerkers	• *Incidentafhandeling (registreren en evalueren).* • *Technisch aanspreekpunt voor IBP-incidenten.* • *Uitvoeren taken conform gegeven richtlijnen en procedures.* • *Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden.*
	Toezicht naleving en communicatie	
	FG Directeuren / Teamleiders	• *Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan* • *Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers* • *Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid* • *Implementeren IBP-maatregelen* • *periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.*
	Opmerking: *in een aantal gevallen is ook de (G)MR hierbij betrokken.*	

De uitwerking van de rollen en taken staan beschreven in bijlage 2.

Bijlage 1: Ondersteunende richtlijnen en procedures

Deze bijlage bevat een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Een aantal zijn vanuit de Algemene Verordening Gegevensbescherming verplicht.

Documenten:	**Aandachtspunten**:
Procedure toestemming gebruik beeldmateriaal	(toestemmingsbrief)
Procedure voor verwijderen van gegevens	(bewaartermijnen)
Communicatie rechten betrokkenen	(communicatie richting betrokkenen)
Procesbeschrijving rechten betrokkenen	(proces rondom aanvragen van betrokkenen)
Privacyreglement	
Autorisatiematrix	(wie mogen gegevens inzien, bewerken enz.)
Afspraken gebruik sociale media	
Procedure rondom training medewerkers	(bewustzijn creëren)
Cameratoezicht	
Wachtwoordbeleid	
Responsible disclosure	
Gedragscode ict en internetgebruik	
Acceptable use policy	(verantwoord gebruik bedrijfsmiddelen)
Procedure rondom uitwisselen gegevens	(passend onderwijs, leerling dossiers, leerplicht enz)
Verplicht vanuit de AVG:	
Procesbeschrijving melden datalekken	
Registratie beveiligingsincidenten	
Dataregister om te voldoen aan de registratieplicht	
Verwerkersovereenkomsten	(privacy bijlage beschikbaar stellen)
Procedure gegevensbeschermingseffectbeoordeling	(DPIA)
Risicoanalyse	
Functionaris voor Gegevensbescherming	(communicatie hierover richting medewerkers)

Bijlage 2: Organisatie; wie doet wat

Deze bijlage beschrijft hoe IBP op drie niveaus wordt georganiseerd.

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

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij Elevantio voor elk niveau een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.

Richtinggevend

Eindverantwoordelijke
Het College van Bestuur is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast.
De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd.
De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de teamleider BMO (verantwoordelijke IBP).

Sturend

Teamleider BMO (verantwoordelijke IBP)
De teamleider BMO heeft een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke (het college van bestuur) en stuurt de mensen aan op uitvoerend niveau. De teamleider BMO moet:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- De uniformiteit bewaken binnen Elevantio
- Het aanspreekpunt zijn (voor incidenten) op het gebied van informatiebeveiliging en privacy
- De verdere afhandeling van incidenten binnen Elevantio coördineren

Functionaris voor Gegevensbescherming
De functionaris voor gegevensbescherming (FG), houdt binnen Elevantio toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG zorgt voor het verbeteren en stimuleren van bewustwording rondom IBP, het afhandelen van informatiebeveiligingsincidenten, adviseert over het regelen van privacy, onderhoudt zo nodig de contacten met de Autoriteit Persoonsgegevens (AP) en rapporteert aan de eindverantwoordelijke (het bestuur). De FG heeft regelmatig overleg met Teamleider BMO. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

BICT / ICT beheer (intern en extern)
Adviseert de teamleider BMO en/of het college van bestuur en is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen Elevantio.

Domeinverantwoordelijke / proceseigenaar
Binnen de school zijn er verschillende domeinen/processen, zoals ict, personeel (HRM, P&O), administratie, facilitaire- en financiële zaken, onderwijs et cetera. Op elk van deze domeinen/processen is

iemand verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

Deze proceseigenaar is tevens verantwoordelijk voor de risico's die veroorzaakt worden doordat personen of applicaties ten onrechte toegang krijgen tot applicaties. Om deze risico's te verkleinen hebben proceseigenaren de volgende specifieke taken:

- Samen met de eindverantwoordelijke stellen zij het beleid voor toegang (autorisaties) vast.
- Samen met BICT/ICT-beheer (intern en extern) zien zij erop toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn en voor hun werkzaamheden toegang toe moeten hebben.
- Samen met functioneel beheer en BICT/ICT-beheer (intern en extern) beoordelen zij periodiek de toegangsrechten van de gebruikers.

Uitvoerend

BICT/ICT beheer (intern en extern)
BICT/ICT beheer (intern en extern) vormt een technisch aanspreekpunt als het gaat over informatiebeveiliging voor het management en de medewerkers.

Ieder softwarepakket of (web-)applicatie heeft een functioneel applicatiebeheerder. Bij vragen over de software of applicatie is bekend wie daarvoor aangesproken kan worden.

Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de medezeggenschap)

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

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

Directeuren/teamleiders hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

Werkgroep AVG:
De werkgroep AVG heeft de volgende opdracht:

- Het signaleren en registreren van alle privacy verzoeken, beveiligingsincidenten en datalekken. Het coördineren van de maatregelen en het toezien op de oplossing van problemen die tot incidenten hebben geleid of waardoor de incidenten zijn veroorzaakt (of het bieden van ondersteuning daarbij);
- Het geven van voorlichting en het doen van algemene aanbevelingen aan de organisatie door het verspreiden van informatie;
- Het leveren van managementrapportages en verbetervoorstellen aan de domeinverantwoordelijke/proceseigenaren over de beveiligingsincidenten en verzoeken tot uitoefening privacyrechten van de betrokkenen.

Bij een calamiteit kan de werkgroep AVG terstond bij elkaar worden geroepen op initiatief van de teamleider BMO. Het doel hiervan is om de **continuïteit** van de informatievoorziening en de privacy te waarborgen. Onder calamiteiten worden verstaan:

- Datalek;
- Grote verstoringen van het netwerk (bijvoorbeeld DDoS aanval);
- Natuurrampen (brand, overstroming, storm, etc.).

De werkgroep AVG behandelt meldingen vertrouwelijk en verstrekt alleen informatie over beveiliging en privacy incidenten als dat noodzakelijk en relevant is voor de oplossing van een incident. De werkzaamheden van de werkgroep AVG zijn gedocumenteerd.

Bijlage 3: Regeling taken en bevoegdheden Functionaris Gegevensbescherming

Artikel 1: definities

a. AVG: Algemene Verordening Gegevensbescherming;
b. FG: functionaris voor gegevensbescherming artikel 37 van de AVG;
c. Verwerkingsverantwoordelijke: het college van bestuur van Stichting Elevantio;
d. Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, bedrijf, organisatie, een dienst of een ander orgaan die/dat ten behoeve van de Verwerkingsverantwoordelijke persoonsgegevens verwerkt;
e. Persoonsgegeven: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (betrokkene) waarbij als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;
f. Verwerking van persoonsgegevens: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;
g. Personeel: medewerkers in loondienst en/of extern ingehuurde medewerkers die in opdracht van de Verwerkingsverantwoordelijke werkzaamheden verrichten.

Artikel 2: Taken

1. De FG heeft de volgende taken:
    a. het houden van toezicht op verwerkingen van persoonsgegevens;
    b. toezicht op wijzigingen in bestaande verwerkingen en/of het aanleggen van nieuwe verwerkingen met persoonsgegevens binnen Elevantio;
    c. geven van (ongevraagd) advies en doen van aanbevelingen over privacy in het algemeen en de toepassing van de AVG;
    d. overleg met (de contactpersoon van) de Autoriteit Persoonsgegevens;
    e. organiseren, inrichten en/of onderhouden van het verwerkingsregister met alle verwerkingen persoonsgegevens binnen Elevantio;
    f. jaarlijks opstellen van een verslag van zijn werkzaamheden;
    g. het (laten) afhandelen van klachten inzake privacy;
    h. overige door het college van bestuur van Elevantio aan de FG opgedragen werkzaamheden aangaande privacy.

2. Het personeel meldt bij de FG alle (nieuwe) verwerkingen van persoonsgegevens alsmede eventuele incidenten met betrekking tot privacy.

Artikel 3: Bevoegdheden

1. De FG is bevoegd, zo nodig met medeneming van de benodigde apparatuur, elke plaats in de gebouwen op de terreinen die bij Elevantio in gebruik zijn en waar persoonsgegevens worden verwerkt, te betreden.
2. De FG is bevoegd inlichtingen te vorderen van een ieder die onder gezag of in opdracht van Elevantio werkzaam is of overeenkomstig voor of namens Elevantio persoonsgegevens verwerkt.
3. De FG is bevoegd inzage te vorderen van zakelijke gegevens en bescheiden waarin persoonsgegevens zijn verwerkt.
4. De FG is bevoegd van de gegevens en bescheiden kopieën te maken.
5. Indien het maken van kopieën niet ter plekke kan gebeuren, is hij bevoegd de gegevens en bescheiden voor maximaal één werkdag mee te nemen.
6. De FG is bevoegd tot het geven van een opdracht tot
    a. het aanmaken van een registratie van persoonsgegevens in overeenstemming met de AVG;
    b. vernietiging van persoonsgegevens, waarvan de bewaartermijn is overschreden of indien de gegevensverwerking onrechtmatig is.
7. De FG is bevoegd zich te laten vergezellen en bijstaan door personen die daartoe door hem zijn aangewezen.
8. De FG maakt van de bevoegdheden als bedoeld in dit artikelen slechts gebruik voor zover dit redelijkerwijs voor de uitoefening van de taak noodzakelijk is. Daarbij is inzage in personeelsdossiers/-systeem te allen tijde in overleg met de teamleider HRM. De FG rapporteert rechtstreeks aan het College van Bestuur over zijn werkzaamheden.

Artikel 4: Weigering

1. Een ieder, die werkzaam is bij en/of in opdracht werkt van de verantwoordelijke, is verplicht aan de FG medewerking te verlenen, die deze redelijkerwijs kan vorderen bij de uitoefening van zijn bevoegdheden.
2. Indien de medewerking aan de uitoefening van de bevoegdheden van de FG zoals bedoeld in artikel 3, wordt geweigerd, kan Elevantio, op een met redenen omkleed verzoek, toestemming verlenen aan de FG de benodigde handelingen zelfstandig uit te voeren in weerwil van de weigering tot medewerking.
3. Het college van bestuur van Elevantio wordt zo spoedig mogelijk in kennis gesteld over de uitvoering van het bepaalde in dit artikel.

Artikel 5: Geheimhouding

1. De FG is verplicht tot geheimhouding van al hetgeen hem op grond van deze regeling bekend is geworden, tenzij de betrokkene in bekendmaking toestemt.

Artikel 6: Regeling

1. Deze regeling wordt vastgesteld en gewijzigd bij besluit van de Verwerkingsverantwoordelijke.
2. Deze regeling treedt in werking op 1 februari 2022 en zal intern aan het personeel bekend worden gemaakt door publicatie op intranet (Digiplein).

Vastgesteld door het college van bestuur van Stichting Elevantio op 31 januari 2022, na instemming van de GMR d.d. 27 januari 2022.

Bijlage 4: Begrippenlijst

Archiefwet
De Archiefwet is een Nederlandse wet die het beheer en de toegang van overheidsarchieven regelt.

Autorisatiematrix
Een schema waarin vast is gelegd wie toegang krijgt tot welke persoonsgegevens. Dat kan op basis van rollen, functies of een mix daarvan.

Autoriteit Persoonsgegevens
De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de wettelijke regels voor de bescherming van persoonsgegevens.

Bestand
Een gestructureerde verzameling persoonsgegevens die via een bepaalde logica toegankelijk is (niet alleen digitaal, maar ook b.v. een archiefkast of geordende verzameling naamkaartjes)

Betrokkenen
De personen van wie persoonsgegevens worden verwerkt.

Bewaartermijnen
De (wettelijke) periode dat een (persoons)gegeven bewaard moet worden.

Data-integriteit
Data-integriteit heeft betrekking op de juistheid van de informatie. Is het niet verouderd of incorrect?

Datalek
Bij een datalek raken persoonsgegevens verloren of worden ze opgeslagen, aangepast, verzonden of op een andere manier verwerkt door iemand die daar geen recht toe heeft. Een datalek is een beveiligingsincident.

Dataminimalisatie
Dataminimalisatie betekent niet meer persoonsgegevens verwerken dan nodig. Gebruik alleen persoonsgegevens die je nodig hebt om je doel te bereiken. Je moet je doel niet met minder persoonsgegevens kunnen bereiken en data niet langer bewaren dan noodzakelijk is. Met andere woorden: kan het minder, dan moet het ook met minder.

Dataregister
Het dataregister is een register van verwerkingsactiviteiten speciaal voor het onderwijs. Het dataregister is voor een gedeelte al ingevuld en van suggesties voorzien.

DDoS
DDoS staat voor ‘Distibuted-denial-of-service’. Pogingen om een computer of netwerk moeilijk bereikbaar te maken door met veel computers tegelijk verzoeken daarop af te vuren.

Derde
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.

Documentatieplicht
De documentatieplicht houdt in dat je vast moet leggen op welke manier je je aan de regels van de AVG houdt.

Doelbinding
Je mag persoonsgegevens alleen gebruiken voor een vooraf vastgelegd doel. Als dat doel niet langer bestaat, moet je de persoonsgegevens vernietigen.

DPIA
DPIA is Data Protection Impact Assessment. In het Nederlands heet het gegevensbeschermingseffectbeoordeling. Met een DPIA onderzoek je wat het effect op de privacy van de betrokkenen is bij het verwerken van persoonsgegevens.

Functionaris voor Gegevensbescherming
Iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de Algemene Verordening Gegevensbescherming (AVG).

Grondslag
De (wettelijke) basis waarop je persoonsgegevens verwerkt. Er zijn 6 mogelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.

Inzage
De mogelijkheid die betrokkenen hebben om hun eigen persoonsgegevens in te zien of een overzicht te krijgen van de persoonsgegevens die worden verwerkt.

ISO
Internationale organisatie voor standaardisatie. Een ISO norm voor informatiebeveiliging is de ISO 27001 of 27002 of 9001.

Kwetsbaarheid
Een fout in de toegangsbeveiliging waardoor onbevoegden toegang krijgen tot software en systemen en mogelijk ongewenste handelingen kunnen uitvoeren. Een kwetsbaarheid kan leiden tot een datalek.

Leveranciers
Aanbieders van ict- of leermiddelen.

Meldplicht datalekken
De plicht tot het doen van een melding doen bij de Autoriteit Persoonsgegevens (AP) zodra er een ernstig datalek geconstateerd is.

Ouders
Waar ouders staat worden de wettelijke vertegenwoordigers bedoeld: personen die de ouderlijke verantwoordelijkheid dragen voor het kind. Dit kunnen ook verzorgenden zijn.

Persoonsgegevens
Alle gegevens waarmee direct of indirect een natuurlijk persoon (mens) kan worden geïdentificeerd. Het kan bijvoorbeeld gaan om een naam, BSN-nummer, geboortedatum, telefoonnummer of IP-adres.

Privacy
Het recht om met rust te worden gelaten, om te weten en te bepalen wat er met gegevens over jou gebeurt en om te weten wie de beschikking heeft over jouw persoonsgegevens.

Profilering
Elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Register van verwerkingsactiviteiten
Een register met informatie over verwerkingen van persoonsgegevens.

Risicoanalyse
Het analyseren van de kans dat een dreiging werkelijkheid wordt en de gevolgen hiervan.

Schoolbestuur
Het schoolbestuur is het bevoegd gezag en daarmee eindverantwoordelijk voor alles dat met IBP te maken heeft.

Transparantie
Helder zijn over de persoonsgegevens die je verzamelt en wat je er mee doet.

Vernietigen
Het definitief verwijderen van gegevens, zodat de persoonsgegevens niet meer aanwezig of terug te halen zijn.

Vertegenwoordiger
Een in de EU gevestigde natuurlijke persoon of rechtspersoon die door de verwerkingsverantwoordelijke of de verwerker is aangewezen om de verwerkingsverantwoordelijke of de verwerker te vertegenwoordigen.

Verwerken
Alles wat er met persoonsgegevens wordt gedaan, wordt in de wet verwerken genoemd. Verwerken is dus onder meer: online en offline persoonsgegevens verzamelen, kopiëren, opslaan, verspreiden, publiceren, delen én uitwisselen. Het maakt dus niet uit wat je doet met persoonsgegevens: alles noemen we verwerken en valt onder de wettelijke bescherming.

Verwerker
Degene of de organisatie die handelt in opdracht van de verwerkingsverantwoordelijke, zoals de leverancier van het leerlingadministratiesysteem. Deze mag alleen verwerkingen doen waarvoor hij uitdrukkelijk opdracht krijgt.

Verwerkingsverantwoordelijke
Degene die het doel en de middelen bepaalt bij het verwerken van persoonsgegevens, zoals een schoolbestuur.