



Informatiebeveiligings- en privacy beleid

Versie: September 2025

Documentgeschiedenis

Revisies

Versie	Datum	Auteur	Review
September 2025	9-09-2025	M. Bildirici	

Vaststelling

Naam	Functie	Versie	Datum
F. El Faraji	Bestuurder	Versie 1.0	8 december 2025
	AVG Kernteam	Versie 1.0	4 december 2025
	GMR	Versie 1.0	18 december 2025

Documentclassificatie

Classificatie	Beschrijving
Openbaar	Dit document mag niet zonder beperkingen worden gedeeld
Vertrouwelijk	Dit document mag worden gedeeld met medewerkers van Stichting El Amal Scholen en ouders.
Geheim	

Inhoudsopgave

1	Inleiding.....	6
1.1	Onze intentie.....	6
1.2	Doelstelling.....	6
1.3	Reikwijdte	7
2	Juridisch kader	7
2.1	Wettelijke en reglementaire kaders	7
2.2	Normen en standaarden.....	8
3	Eigenaarschap en verantwoordelijkheden	8
3.1	Three Lines model	9
3.1.1	Eerste lijn: eindverantwoordelijkheid bij het bestuur.....	9
3.1.2	Tweede lijn: adviseren en ondersteunen	9
3.1.3	Derde lijn: onafhankelijke controle	10
3.2	Medezeggenschap	10
4	Beleidsthema's informatiebeveiliging	10
4.1	Risicomanagement	10
4.2	Kennis en Afhankelijkheid medewerkers.....	11
4.3	Bedrijfscontinuïteit	11
4.4	Back-up en herstel	12
4.5	Fysieke beveiliging	13
4.6	Systeem- en data-eigenaarschap en configuratiebeheer	13
4.7	Classificatie van systemen en data.....	13
4.8	Securitybaseline.....	14
4.9	Bewustwording	15
4.10	Incident- en problemmanagement	15
4.11	Risicomanagement leveranciers.....	16
4.12	Werkplekken en mobiele apparaten	16
4.13	Identiteits- en toegangsbeheer.....	17
4.14	Vulnerabilitymanagement en pentesting	17
4.15	Patchmanagement	17
4.16	Logging	18
4.17	Digitaal sleutelbeheer.....	18

5	Uitgangspunten privacy	20
6	Beleidsthema's privacy	22
6.1	Verwerkingsregister	22
6.1.1	Legitiem doel en doelbinding.....	23
6.1.2	Grondslag.....	23
6.2	Informatieplicht	24
6.3	Toestemming	25
6.4	Privacy by design en privacy by default	25
6.4.1	Dataminimalisatie	26
6.5	Bewaartermijnen	26
6.6	Afhandelen van datalekken	26
6.7	Data Protection Impact Assessment	27
6.8	Uitwisseling persoonsgegevens.....	27
6.9	Rechten van betrokkenen	28
7	Verantwoording IBP	29
7.1	Naleving AVG.....	29
7.2	Rapportage.....	29
7.3	Beleidsherziening	29

1 Inleiding

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. Lesmateriaal wordt digitaal aangeboden, toetsingsprogramma's worden digitaal en de resultaten en ontwikkelingen van leerlingen worden opgenomen in een digitaal leerlingvolgsysteem. Daarnaast wordt ook veel gebruikgemaakt van digitale communicatie tussen de school, leerlingen en ouders/verzorgers. Door deze ontwikkelingen neemt het risico op verstoring van het onderwijs, verlies of misbruik van gegevens en overmatige dataverzameling toe. Het is de verantwoordelijkheid van de Stichting el Amal om dat te voorkomen en een veilige leeromgeving te bieden.

Dit beleid voor informatiebeveiliging en privacy (IBP-beleid) beschrijft hoe Stichting el Amal omgaat met de beveiliging van informatie en hoe de verwerking van (persoons)gegevens wordt gewaarborgd en gehandhaafd. In het beleid worden de verschillende rollen en verantwoordelijkheden binnen Stichting el Amal op het gebied van informatiebeveiliging en privacy (IBP) beschreven.

1.1 Onze intentie

Stichting el Amal Scholen draagt de verantwoordelijkheid voor het creëren van een veilige werk- en leeromgeving. Dit houdt in dat Stichting el Amal passende technische en organisatorische maatregelen toepast om informatie te beschermen en ongeoorloofde toegang, verlies of misbruik te voorkomen. Het recht op privacy is een grondrecht. Iedereen heeft recht op privacy en bescherming van de persoonlijke levenssfeer. Dit geldt vanzelfsprekend ook voor leerlingen, ouders/verzorgers, medewerkers en docenten. Stichting el Amal is verantwoordelijk voor het waarborgen van de privacy van de leerlingen en het personeel. Dit betekent ook dat deze betrokkenen zeggenschap hebben over het gebruik van hun persoonsgegevens, zoals wettelijk bepaald. Bij Stichting el Amal staat het bieden van goed onderwijs voorop. Om dit te kunnen doen verwerken wij diverse persoonsgegevens van leerlingen, ouders/verzorgers, medewerkers en docenten. Stichting el Amal vindt het belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. Het goed regelen van informatiebeveiliging en privacy in een beleid is noodzakelijk om de gevolgen van mogelijke informatiebeveiliging- en privacyrisico's tot een aanvaardbaar niveau terug te brengen en de voortgang van het onderwijs te kunnen waarborgen.

1.2 Doelstelling

Dit IBP-beleid is erop gericht de kwaliteit van de verwerking van (persoons)gegevens en de beveiliging van informatie en systemen te verhogen. Hierbij moet een juiste balans bestaan tussen veiligheid, privacy en functionaliteit. Het uitgangspunt is dat een veilige werk- en leeromgeving wordt gecreëerd, de persoonlijke levenssfeer van de betrokkenen wordt gerespecteerd en Stichting el Amal voldoet aan relevante wet- en regelgeving. Dit gebeurt onder andere door bewustwording te vergroten over het belang van het zorgvuldig omgaan met informatie, systemen en persoonsgegevens.

Stichting el Amal maakt gebruik van het 'Normenkader Informatiebeveiliging en Privacy voor het onderwijs' - oftewel het Normenkader IBP - om inzichtelijk te maken waar de organisatie nu staat en

welke maatregelen genomen moeten worden om een veilige werkomgeving te creëren en te voldoen aan de AVG.

1.3 Reikwijdte

Dit beleid is van toepassing op alle leerlingen, docenten, medewerkers, bezoekers, ouders/verzorgers, derde partijen en andere gebruikers die toegang hebben tot of werken met de informatie van Stichting el Amal. Het beleid heeft betrekking op de verwerking van alle soorten gegevens en informatie waaronder; persoonsgegevens, bedrijfsinformatie en technische gegevens. Het is van toepassing op alle gegevensverwerkingen die onder de AVG vallen.

Informatiebeveiliging en privacy maken integraal onderdeel uit van dit IBP-beleid. Informatiebeveiliging is een belangrijke voorwaarde voor privacy. Informatiebeveiliging omvat de beveiliging van *alle* informatie, terwijl privacy gaat over de verwerking van persoonsgegevens.

2 Juridisch kader

2.1 Wettelijke en reglementaire kaders

Het juridisch kader voor dit IBP-beleid wordt gevormd door de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet UAVG. Daarnaast kunnen uit andere wet- en regelgeving verplichtingen of instructies voortvloeien voor de verwerking van persoonsgegevens. Voor Stichting el Amal is op dit gebied onder andere de volgende wetgeving van belang:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra
- Wet onderwijstoezicht
- Archiefwet en Archiefbesluit
- Leerplichtwet
- Wet medezeggenschap op scholen
- Arbeidsregelgeving en CAO
- Belastingwetgeving
- Telecommunicatiewet en e-privacy wetgeving

Indien een (mogelijke) strijdigheid tussen dit beleid en de AVG en/of gerelateerde wet- en regelgeving bestaat, dan moet voorafgaand aan een verwerking overlegd worden met de afdeling Juridische zaken en de privacy officer.

2.2 Normen en standaarden

Als onderwijssector hebben we afgesproken om toe te werken naar één normenkader om aan de minimale vereisten te voldoen voor digitaal veilig onderwijs. Dit is het 'Normenkader

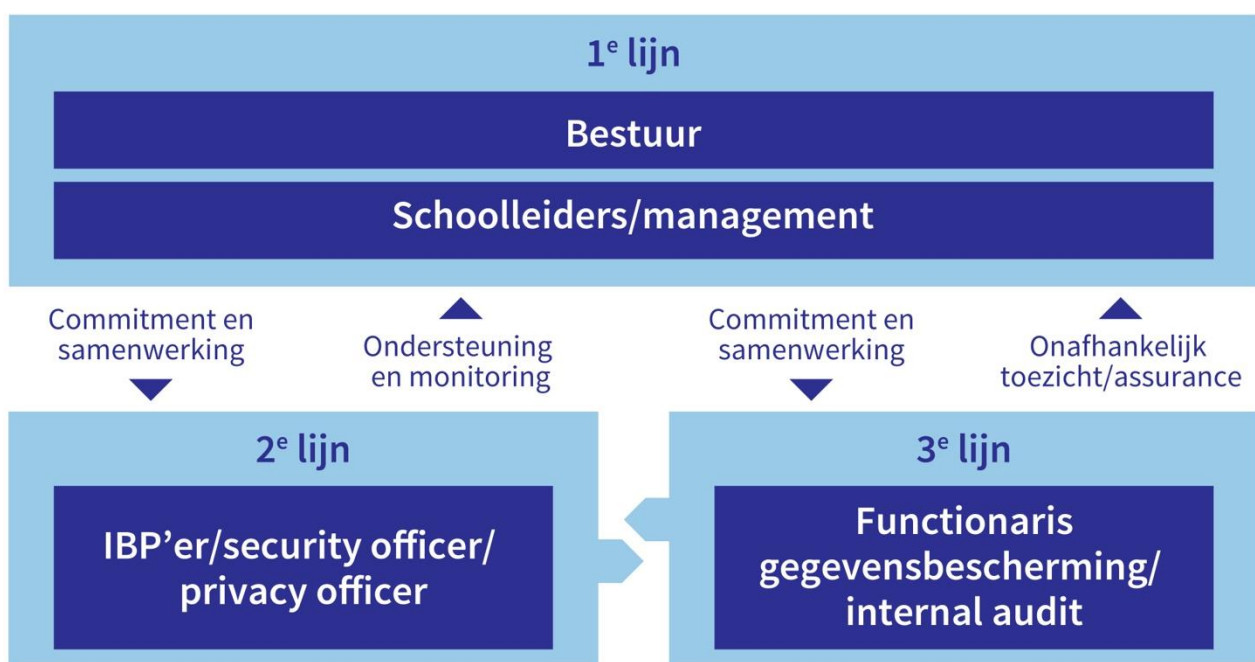
Informatiebeveiliging en Privacy voor het onderwijs'. Dit normenkader beschrijft de regels, principes en standaarden op het gebied van informatiebeveiliging en privacy waaraan Stichting el Amal moet voldoen voor een digitale veilige schoolomgeving.

3 Eigenaarschap en verantwoordelijkheden

- *We maken gebruik van het Three Lines model. Dat is een organisatiemodel dat helpt om de governance van je organisatie op een gestructureerde manier te organiseren.*

Dit hoofdstuk beschrijft hoe de verschillende rollen en verantwoordelijkheden met betrekking tot informatiebeveiliging en privacy samenhangen.

3.1 Three Lines model



Informatiebeveiliging en privacy bij Stichting el Amal is ingericht volgens het Three Lines model (3L-model). Het 3L-model is een leidraad bij het inrichten van de governance van een organisatie.

3.1.1 Eerste lijn: eindverantwoordelijkheid bij het bestuur

Het 3L-model heeft als uitgangspunt dat de eerste lijn verantwoordelijk is voor processen, informatie en systemen van de organisatie, de risico's die hieruit voortvloeien en het treffen van de juiste maatregelen om de risico's te verkleinen. De eerste lijn bestaat uit het bestuur, schoolleiders, en het verdere lijnmanagement van Stichting el Amal. De PO'er en IT'er worden betrokken bij de eerste lijn. Het bestuur is binnen de eerste lijn eindverantwoordelijk voor informatiebeveiliging en privacy, maar kan bepaalde verantwoordelijkheden beleggen bij andere functies binnen de organisatie. Bij de

beschrijving van de beleidsthema's in hoofdstuk 4 en 6 wordt per thema beschreven wie er verantwoordelijk is.

3.1.2 Tweede lijn: adviseren en ondersteunen

Naast de eerste lijn moet er een rol zijn die de eerste lijn ondersteunt, adviseert, coördineert en die bewaakt of het management de verantwoordelijkheden ook daadwerkelijk neemt. Dit is de tweede lijn. De tweede lijn bestaat uit privacy officers, IBP-adviseurs en IT'er.

3.1.3 Derde lijn: onafhankelijke controle

De derde lijn controleert of de eerste en tweede lijn soepel samenwerken en goed functioneren. De derde lijn is onafhankelijk, opereert los van de andere organisatieonderdelen en suggereert waar nodig verbeteringen. De functionaris gegevensbescherming (FG) en de interne auditor vallen binnen de derde lijn. De FG wordt aangesteld door het bestuur en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een reglement dat door het bestuur wordt vastgesteld.

3.2 Medezeggenschap

Stichting el Amal betreft de medezeggenschapsraad (MR) bij besluiten over regelingen en procedures ten aanzien van de bescherming van persoonsgegevens. Het schoolbestuur is eindverantwoordelijk voor het informeren van de medezeggenschapsraad en voor het opstellen van instemmingsprocedures.

4 Beleidsthema's informatiebeveiliging

In hoofdstuk 4 zijn de beleidsthema's op het gebied van informatiebeveiliging opgenomen.

4.1 Risicomanagement

Toelichting

- *Het Risicomanagementbeleid is in een apart voorbeelddocument beschreven.*

Stichting el Amal hanteert een losstaand Risicomanagementbeleid. Zie bijlage Het risicomanagementbeleid Stichting el Amal.

4.2 Kennis en Afhankelijkheid medewerkers

Stichting el Amal is voor de beveiliging van informatie en de continuïteit van het onderwijs afhankelijk van de kennis en beschikbaarheid van medewerkers. Stichting el Amal wil voorkomen dat er onvoldoende kennis aanwezig is bij medewerkers of dat kritieke kennis en vaardigheden onvoldoende aanwezig zijn binnen de organisatie. Taken van sleutelfiguren moeten daarom altijd overgenomen kunnen worden door andere medewerkers. Hiervoor hanteert Stichting el Amal de volgende maatregelen:

- Een back-upplan voor kritieke medewerkers.
- Voldoende training en certificering.
- Een indienst-/uitdiensttredingproces waarin rekening gehouden wordt met aansluiting op het proces voor het beheren van rechten en rollen, de overdracht van kennis en documentatie en screening van medewerkers.

Verantwoordelijkheden:

- Functioneel bestuurder Stichting El Amal is verantwoordelijk voor het formeel goedkeuren van het back-upplan voor kritieke medewerkers.
- Functioneel bestuurder Stichting El Amal (ism de schooldirectie) is verantwoordelijk voor het opstellen en het beheren van het back-upplan voor kritieke medewerkers.
- Functioneel bestuurder Stichting El Amal is verantwoordelijk voor het opstellen en het beheren van het indienst/ uitdiensttreding proces. Dit gebeurt in samenwerking met het AVG- kernteam en de schooldirectie. AVG-kernteam voor technische kant van informatiebeveiliging & Privacy en de schooldirectie voor de uitvoering en afronden van het proces.

4.3 Bedrijfscontinuïteit

Stichting el Amal zorgt ervoor dat mogelijke verstoringen van het onderwijs zo snel mogelijk verholpen worden en dat de impact van verstoringen beperkt blijft. Door processen te analyseren worden de meest kritieke applicaties en medewerkers geïdentificeerd, en wordt bepaald welke terugvalopties nu aanwezig zijn. Hierna kunnen maatregelen geïmplementeerd worden om verstoringen zo veel mogelijk te voorkomen of de impact te beperken. Er is een crisismanagementteam (kernteam AVG) aanwezig om snel en adequaat op incidenten te reageren.

Stichting el Amal hanteert de volgende maatregelen voor bedrijfscontinuïteit:

- **Business impact analyses (BIA) op basis van de processen van de organisatie.** De processen worden op basis van een risicogestuurde aanpak geanalyseerd, waarbij eerst de meest kritieke processen behandeld worden. Nieuwe risico's die tijdens deze BIA's geïdentificeerd zijn, worden opgenomen in het risicoregister (YSN). Zie hiervoor het risicomanagementbeleid.
- **Een bedrijfscontinuïteitsplan (BCP).** Een crisismanagementaanpak waaronder periodieke crisisoefeningen maken onderdeel uit van het BCP. Taken en verantwoordelijkheden zijn duidelijk toegewezen in het BCP. Het BCP wordt na een jaarlijkse oefening steeds geactualiseerd.

Verantwoordelijkheden:

- Functioneel bestuurder Stichting El Amal is verantwoordelijk voor het formeel goedkeuren van het bedrijfscontinuïteitsplan. De uitvoering wordt belegd bij IT-beheerder
- Functioneel bestuurder Stichting El Amal en het AVG-kernteam zijn verantwoordelijk voor het opstellen en het beheren van het bedrijfscontinuïteitsplan.

4.4 Back-up en herstel

Om de impact van verstoringen of dataverlies te beperken zorgt Stichting el Amal voor back-ups van systemen en data. Op basis van de BIV-classificatie van systemen worden de back-upvereisten voor de systemen en de data binnen deze systemen vastgesteld. Back-ups worden regelmatig getest om te verifiëren of gegevens kunnen worden hersteld binnen de vastgestelde periode. De volgende uitgangspunten worden hierbij gehanteerd:

- De proceseigenaar is degene die beslist over de continuïteitsvereisten van een dataverwerking of een systeem. Het initiatief voor deze afweging komt van de systeemeigenaar.
- We stellen dezelfde back-upeisen aan diensten van externe leveranciers als aan systemen die we zelf beheren.
- Bij voorkeur maken we bij externe leveranciers gebruik van de back-upfaciliteit die ze zelf bij hun dienst aanbieden. Ontbreekt die of voldoet die niet, dan maken we zelf back-ups van de informatie die we verwerken in de dienst van deze leverancier.
- We evalueren jaarlijks de manier waarop we zelf back-ups maken.

Verantwoordelijkheden:

- Stichting el Amal stelt een procesbeschrijving op voor back-up en herstel.
- IT-verantwoordelijke is verantwoordelijk voor het formeel goedkeuren van de back-up en herstel procesbeschrijving.
- IT-verantwoordelijke is verantwoordelijk voor het opstellen en het beheren van de back-up en herstel procesbeschrijving.
- De systeemeigenaar is verantwoordelijk voor het toepassen van het back-up en herstelproces.

4.5 Fysieke beveiliging

Toelichting

- *Het fysieke beveiligingsbeleid is in een apart voorbeelddocument beschreven.*

Stichting el Amal hanteert een losstaand Fysiek beveiligingsbeleid. Zie Fysiek beveiligingsbeleid Stichting el Amal.

4.6 Systeem- en data-eigenaarschap en configuratiebeheer

Om IT-processen te beheren is inzicht nodig in welke systemen worden gebruikt binnen de organisatie. Veel van de IBP-thema's in dit beleid zijn afhankelijk van dit inzicht. De rol van systeemeigenaar wordt gebruikt om bepaalde verantwoordelijkheden toe te kunnen wijzen die specifiek voor een systeem gelden. De rol van proceseigenaar wordt gebruikt om bepaalde verantwoordelijkheden toe te kunnen wijzen die te maken hebben met een specifiek proces. Stichting el Amal maakt de keuze om eigenaarschap van data niet vast te leggen, maar zich te beperken tot het beleggen van eigenaarschap van systemen waar deze data in is vastgelegd. Voor het vastleggen van processen en het eigenaarschap van systemen en processen treft Stichting el Amal de volgende maatregelen:

- Stichting el Amal heeft een configuratiemanagementdatabase (CMDB) waarin alle systemen, het eigenaarschap en andere benodigde eigenschappen bijgehouden worden.
- Systeemeigenaarschap wordt bepaald vóór implementatie van nieuwe systemen. De eigenaren van systemen worden vastgelegd in het CMDB.
- Proceseigenaarschap wordt bepaald en vastgelegd binnen het verwerkingsregister.

Verantwoordelijkheden:

- IT-verantwoordelijke (samen met Rolf-groep) is verantwoordelijk voor het opstellen en het beheren van de CMDB.
- De systeemeigenaar van elk systeem is verantwoordelijk voor het vastleggen van de juiste eigenschappen in de CMDB.

4.7 Classificatie van systemen en data

Om risicogestuurd beslissingen te kunnen nemen is belangrijk om per systeem het benodigde niveau van beschikbaarheid, integriteit en vertrouwelijkheid (BIV) te bepalen. De classificatie is beperkt tot systeemniveau. Stichting el Amal kiest ervoor om de classificatie niet per individueel dataobject toe te passen. Stichting el Amal heeft voor elk systeem dat opgenomen is in de CMDB een BIV-classificatie uitgevoerd. Deze BIV-classificatie wordt gebruikt om te bepalen welke maatregelen er voor het betreffende systeem geïmplementeerd moeten worden. Voor het goed toepassen van de BIV-classificatie treft Stichting el Amal de volgende maatregelen:

- De BIV-classificatie wordt uitgevoerd vóór de aanschaf van een nieuw systeem. Zie beleidsthema 4.11.
- De BIV-classificatie wordt vastgelegd in de CMDB.

Verantwoordelijkheden:

- De systeemeigenaar van elk systeem is verantwoordelijk voor het uitvoeren van de BIV-classificatie en het vastleggen hiervan in de CMDB.

4.8 Securitybaseline

Een securitybaseline voor IT-systemen is vastgesteld om het risico van ongeoorloofde toegang tot IT-middelen te beperken. Stichting el Amal maakt gebruik van het certificeringsschema ROSA als securitybaseline voor IT-systemen in eigen beheer. De securitybaseline is formeel vastgelegd, wordt periodiek geactualiseerd en wordt goedgekeurd door het schoolbestuur. De toepassing van de securitybaseline voor IT-middelen wordt periodiek beoordeeld op naleving. Afwijkingen van de baselines zijn gedocumenteerd en goedgekeurd.

Verantwoordelijkheden:

- Functioneel bestuurder i.o.m. de ICT'er is verantwoordelijk voor het formeel goedkeuren van de securitybaseline.
- De systeemeigenaar van elk systeem is verantwoordelijk voor het voldoen aan de securitybaseline en het vastleggen van afwijkingen op de baseline.

4.9 Bewustwording

Beleid en technische maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hierin ook een belangrijke factor. Daarom wordt het bewustzijn van medewerkers over de verantwoordelijkheden die ze hebben voortdurend aangescherpt, zodat de kennis van bestaande risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingssessies voor medewerkers, leerlingen en gasten. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de verantwoordelijke IBP, de FG, en de Privacy officer met het Bestuur El Amal als eindverantwoordelijke.

Verantwoordelijkheden:

- Stichting el Amal is verantwoordelijk voor het formeel goedkeuren van het bewustwordingsprogramma.
- PO'er is verantwoordelijk voor het opstellen en het beheren van het bewustwordingsprogramma.

4.10 Incident- en problemmanagement

Incidentmanagement is het proces voor het melden van incidenten binnen de organisatie. Sommige incidenten kunnen een datalek tot gevolg hebben. Incidenten binnen de organisatie zijn nooit helemaal uit te sluiten.

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 bij privacy@elamalscholen.nl. AVG-kern team maakt de melding in YSN register.

Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

Een helder beschreven incidentmanagementproces is aanwezig om incidenten op tijd te herkennen en ze adequaat af te handelen. De manier waarop dat gebeurt is vastgelegd in een procesbeschrijving waarbij de volgende onderwerpen minimaal terugkomen:

- **Een centraal punt** voor het melden van incidenten.
- **Incidentenregister:** Binnen dit incidentenregister wordt er duidelijk onderscheid gemaakt tussen datalekken en andere type incidenten.

- **De classificatie van incidenten:** Bij elk incident moet worden vastgesteld om wat voor type incident het gaat (beveiliging, privacy, etc.)
- **De afhandeling van het incident:** Het is duidelijk wie bij welk type incident betrokken moeten worden en wie verantwoordelijk is voor het afhandelen van de incidenten.
- **Problemmanagement:** Indien incidenten regelmatig terugkomen worden deze aangemerkt als een *known error*. De procesbeschrijving beschrijft de vervolgstappen voor een terugkerend incident.
- **Monitoren en rapporteren:** Afhandeling van incidenten en problemen worden gemonitord. Hierover wordt periodiek gerapporteerd.

Verantwoordelijkheden:

- Functioneel bestuurder Stichting El Amal is verantwoordelijk voor het formeel goedkeuren van de incidentmanagementprocesbeschrijving.
- PO'er is verantwoordelijk voor het opstellen en het beheren van de incidentmanagementprocesbeschrijving. PO'er voor datalekken en IT voor technische beveiligingsincidenten. AVG team zorgt voor het doorzetten van de gegevens naar YSN.
- IT-verantwoordelijke en PO'er zijn verantwoordelijk voor het inrichten en beheren van het incidentenregister.

4.11 Risicomanagement leveranciers

Stichting el Amal besteedt een deel van de IT uit aan leveranciers, maar blijft eindverantwoordelijk voor beveiliging van informatie en persoonsgegevens. Om ervoor te zorgen dat ook leveranciers zich houden aan de technische maatregelen die volgen uit de securitybaseline zijn bepaalde stappen toegevoegd aan het leveranciersmanagementproces.

- Er is een lijst met maatregelen opgesteld op basis van de securitybaseline van Stichting el Amal. (De uitvoering ligt bij Rolf-groep. Het securitysysteem wordt door Rolf-groep beheerd).
- Er is een leveranciersmanagementproces waar de volgende stappen onderdeel van zijn:
 - Voor de aanschaf van een nieuw systeem wordt een BIV-classificatie uitgevoerd.
 - Op basis van deze BIV-classificatie en de lijst met maatregelen worden aanbestedingseisen opgesteld.
 - Er wordt een periodieke controle gedaan op het voldoen aan de aanbestedingseisen.

Verantwoordelijkheden:

- IT-verantwoordelijke is verantwoordelijk voor het formeel goedkeuren van de leveranciersmanagementprocesbeschrijving.
- IT-verantwoordelijke is verantwoordelijk voor het opstellen en het beheren van de leveranciersmanagementprocesbeschrijving.
- De systeemeigenaar is verantwoordelijk voor de periodieke controle op het voldoen aan de aanbestedingseisen.

4.12 Werkplekken en mobiele apparaten

Persoonsgegevens en andere informatie uit systemen die binnen onze organisatie worden gebruikt, worden ontsloten via verschillende apparaten zoals laptops, tablets, smartphones en desktop-pc's. Deze apparaten brengen risico's met zich mee op het gebied van beveiliging, dataverlies en compliance. Daarom treft Stichting el Amal de volgende maatregelen:

- Stichting el Amal hanteert een richtlijn voor het gebruik van werkplekken en mobiele apparaten.

Verantwoordelijkheden:

- Functioneel bestuurder Stichting El Amal is verantwoordelijk voor het formeel goedkeuren van de richtlijn voor het gebruik van werkplekken en mobiele apparaten.
- Schooldirectie is verantwoordelijk voor het opstellen en het beheren van de richtlijn voor het gebruik van werkplekken en mobiele apparaten. Momenteel werken we aan een gezamenlijk overeenkomst voor alle medewerkers. Voor alle scholen geldt dezelfde regels.
- AVG-kern team is verantwoordelijk voor het opstellen van de richtlijnen en de schooldirectie voor de uitvoering.

4.13 Identiteits- en toegangsbeheer

Toelichting

- *Het Identiteits- en toegangsbeheer (IAM) beleid is in een apart voorbeelddocument beschreven.*

4.14 Vulnerabilitymanagement en pentesting

Vulnerabilitymanagement en pentesting vormen een essentieel onderdeel voor het verminderen van risico's, het voorkomen van ongeautoriseerde toegang tot IT-systemen en het beschermen van gegevens tegen mogelijke dreigingen.

4.15 Patchmanagement

Met patchmanagement verhelp je kwetsbaarheden in systemen, applicaties en hardware. Het doel is om de beveiliging, stabiliteit en prestaties van IT-omgevingen te waarborgen door het tijdig testen en implementeren van patches. Hiervoor neemt stichting el Amal Scholen de volgende maatregel:

- Stichting el Amal Scholen heeft een proces voor het inrichten van patchmanagement.

Verantwoordelijkheden:

- Functioneel bestuurder is voor het formeel goedkeuren van de procesbeschrijving patchmanagement.
- PO'er en ICT'er zijn verantwoordelijk voor het opstellen en het beheren van de procesbeschrijving patchmanagement.

- De systeemeigenaar is verantwoordelijk voor tijdig testen en implementeren van patches.

4.16 Logging

Loggegevens bieden inzicht in de activiteiten van systemen en spelen een sleutelrol bij het detecteren, onderzoeken en voorkomen van beveiligingsincidenten. Om loggegevens vast te leggen neemt Stichting el Amal de volgende maatregel:

- Stichting el Amal heeft een procesbeschrijving voor het vastleggen van loggegevens binnen systemen.
- Login en monitoring door de ICT-afdeling van stichting El Amal 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.

Verantwoordelijkheden:

- Functioneel bestuurder Stichting el Amal is verantwoordelijk voor het formeel goedkeuren van de procesbeschrijving voor logging.
- IT-verantwoordelijke is verantwoordelijk voor het opstellen en het beheren van de procesbeschrijving voor logging.

4.17 Digitaal sleutelbeheer

Rolf-groep gebruikt encryptie voor de volgende doeleinden:

- **Bescherming van vertrouwelijke gegevens:** Door het toepassen van sterke versleutelingstechnieken bij opslag, verzending en verwerking van gegevens.
- **Verificatie van identiteit:** Gebruik van cryptografische methoden zoals digitale handtekeningen en certificaten om betrouwbare communicatie te waarborgen.
- **Waarborgen van gegevensintegriteit:** Detecteren van wijzigingen in gegevens.

Om encryptie toe te passen treft Stichting el Amal de volgende maatregel:

- Rolf-groep hanteert een procesbeschrijving voor het beheer van digitale sleutels.

Verantwoordelijkheden:

Uitbesteed aan Rolfgroep

- Rolfgroep is verantwoordelijk voor het formeel goedkeuren van de procesbeschrijving digitaal sleutelbeheer.
- Rolfgroep is verantwoordelijk voor het opstellen en het beheren van de procesbeschrijving voor digitaal sleutelbeheer.

5 Uitgangspunten privacy

Het algemene uitgangspunt in dit IBP-beleid is dat persoonsgegevens in overeenstemming met de AVG en gerelateerde wet- en regelgeving op zorgvuldige wijze worden verwerkt. Om aan dit uitgangspunt te voldoen verwerkt Stichting el Amal persoonsgegevens in overeenstemming met de privacyvuistregels die in verderop in dit hoofdstuk worden uiteengezet. Stichting el Amal treft verdiepende maatregelen om de beleidsthema's in dit IBP-beleid in te vullen.

Persoonsgegevens

Persoonsgegevens zijn gegevens die direct of indirect over iemand gaan en dus naar een persoon te herleiden zijn, zoals een naam of e-mailadres. Naast gewone persoonsgegevens - denk aan contactgegevens en onderwijsnummers - onderscheidt de AVG bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens. Daarnaast bestaat een categorie 'gevoelige' persoonsgegevens die niet expliciet in de AVG is benoemd. Dit zijn persoonsgegevens die vanwege hun aard privacygevoelig zijn en daarom extra bescherming verdienen.

- **Bijzondere persoonsgegevens** zijn gegevens die te maken hebben met bijvoorbeeld ras of etnische afkomst, gezondheid, religie of seksueel gedrag. De verwerking van deze gegevens is verboden, tenzij een wettelijke uitzondering bestaat zoals toestemming van de betrokkene.
- **Strafrechtelijke gegevens** zijn gegevens die te maken hebben met strafrechtelijke veroordelingen en strafbare feiten. De verwerking van deze gegevens is ook verboden, tenzij hiervoor een wettelijke uitzondering geldt.
- **Gevoelige persoonsgegevens** zijn gegevens die een groter privacyrisico vormen dan gewone persoonsgegevens. Denk aan financiële gegevens, burgerservicenummers (BSN), beoordelingen of gegevens van kwetsbare leerlingen.

NB: Nummers ter identificatie van een persoon, zoals het BSN, mogen alleen worden gebruikt voor specifieke doeleinden die in de wet zijn vastgelegd. Een onderwijsnummer (persoonsgebonden nummer) is gelijk aan het BSN.

Privacyvuistregels

Bij het verwerken van persoonsgegevens houdt Stichting el Amal rekening met onderstaande vuistregels. Door deze basisprincipes te volgen zorgen we ervoor dat we kunnen voldoen aan de AVG.

1. We verwerken persoonsgegevens rechtmatig en transparant

Stichting el Amal verzamelt en gebruikt persoonsgegevens op een eerlijke en transparante manier. Persoonsgegevens worden alleen verwerkt als daarvoor een wettelijke grondslag bestaat in de AVG. We leggen altijd duidelijk uit waarom we bepaalde gegevens nodig hebben, wat we ermee doen en hoe lang we deze gegevens bewaren. Daarom informeren we ouders en leerlingen tijdig over het gebruik van hun persoonsgegevens, via een transparante privacyverklaring. Dit gebeurt bijvoorbeeld op het moment van inschrijving van een leerling.

2. We verwerken persoonsgegevens voor specifieke doeleinden

Stichting el Amal verwerkt persoonsgegevens alleen wanneer vooraf de specifieke doeleinden voor de verwerking zijn bepaald. Deze doeleinden worden vastgelegd. Persoonsgegevens worden niet voor andere, niet-verenigbare, doelen verwerkt. We zullen dus niet persoonsgegevens verzamelen omdat die wellicht ooit van pas gaan komen. We doen dit alleen met vooraf bepaalde, duidelijke en gerechtvaardigde doelen, zoals het plannen van onderwijs en communiceren met leerlingen en ouders over de voortgang en schoolactiviteiten.

3. We verwerken alleen noodzakelijke persoonsgegevens

Stichting el Amal verzamelt alleen persoonsgegevens die noodzakelijk zijn voor het doel waarvoor ze worden verwerkt. We vragen dus niet om meer gegevens dan we daadwerkelijk nodig hebben en hanteren hierbij het uitgangspunt 'zo min mogelijk'. We onderzoeken altijd of we met minder gegevens of enkel met anonieme gegevens kunnen werken. Zo vragen we bij de inschrijving van een leerling alleen om de gegevens die relevant zijn voor het kunnen bieden van onderwijs en bewaren we geen overbodige gegevens die niet nodig zijn voor onze schoolactiviteiten.

4. We zorgen dat persoonsgegevens juist en actueel zijn

Stichting el Amal treft maatregelen om ervoor te zorgen dat persoonsgegevens correct en actueel zijn. Onjuiste of achterhaalde gegevens worden geactualiseerd of verwijderd. Leerlingen en ouders kunnen op een laagdrempelige manier doorgeven dat persoonsgegevens incorrect zijn en/of gewijzigd moeten worden. Onze processen en systemen worden zo ingericht dat de juistheid van gegevens zoveel mogelijk wordt afgedwongen en gecontroleerd.

5. We bewaren persoonsgegevens niet langer dan nodig

Stichting el Amal bewaart persoonsgegevens niet langer dan noodzakelijk is voor het doel waarvoor ze zijn verzameld. Zodra gegevens niet meer nodig zijn, worden ze verwijderd of geanonimiseerd. We houden ons hierbij aan vooraf vastgestelde bewaartermijnen. Zo wordt het leerlingendossier (inclusief rapporten en schoolprestaties) na uitschrijving van een leerling niet langer bewaard dan nodig is voor administratieve en onderwijsdoeleinden en dus zo spoedig mogelijk verwijderd, in ieder geval binnen 2 jaar na uitschrijving.

6. We zorgen voor een passende bescherming van persoonsgegevens

We kunnen de privacy van leerlingen, ouders en medewerkers alleen goed beschermen als we op een veilige manier met hun persoonsgegevens omgaan. We zijn daarom verantwoordelijk voor het treffen van passende technische en organisatorische beveiligingsmaatregelen. Die maatregelen moeten ervoor zorgen dat de persoonsgegevens op een passende wijze worden beveiligd en worden beschermd tegen verlies, vernietiging, beschadiging of onrechtmatige verwerking. Dit doen we bijvoorbeeld door het

gebruik van veilige systemen voor de opslag van leerlinggegevens en het opleiden van personeel in het veilig omgaan met gevoelige gegevens.

7. We kunnen aantonen dat we voldoen aan de AVG

We zijn verantwoordelijk voor het naleven van bovengenoemde vuistregels en kunnen daarmee aantonen dat we voldoen aan de belangrijkste uitgangspunten van de AVG. Dit doen we bijvoorbeeld door het bijhouden van een verwerkingsregister en het uitvoeren van *Data Protection Impact Assessments* (DPIA's) voor gegevensverwerkingen met een hoog privacyrisico.

8. We kunnen ons ethisch verantwoorden

Bij het beoordelen van verwerkingen van persoonsgegevens houdt Stichting el Amal niet alleen rekening met de vereisten uit de AVG ('*mogen we dit?*'), maar nadrukkelijk ook met ethische aspecten ('*willen we dit?*'). Het gaat hierbij dus niet om de vraag of we iets 'mogen' of 'kunnen', maar juist om de vraag of we iets zouden moeten 'willen' als school. Ethische aspecten spelen in het bijzonder een rol bij verwerkingen die privacyrisico's kunnen opleveren, bijvoorbeeld bij het gebruik van meekijksoftware of schermcontroles. Dit moet ook worden gezien vanuit een ethisch afwegingskader. We stellen ons dan ook eerst de vraag of we het kunnen uitleggen aan leerlingen en ouders.

6 Beleidsthema's privacy

6.1 Verwerkingsregister

Stichting el Amal heeft maatregelen getroffen om aantoonbaar te voldoen aan de eisen uit de AVG. Dit houdt onder meer in dat Stichting el Amal kan aantonen dat de verwerking van persoonsgegevens voldoet aan de uitgangspunten uit de AVG. Stichting el Amal geeft onder meer invulling aan haar verantwoordingsplicht door een overzicht bij te houden met informatie over de persoonsgegevens die zij verwerkt. Dit heet het verwerkingsregister. Dit register bevat bijvoorbeeld informatie over de leerlingenadministratie of het HR-systeem. Het bijhouden van het verwerkingsregister zorgt voor een goed overzicht van welke persoonsgegevens worden verwerkt en met welk doel dit gebeurt. Het register stelt Stichting el Amal in staat te voldoen aan haar verantwoordingsplicht.

Het verwerkingsregister bevat van afzonderlijke verwerkingsactiviteiten informatie over onder meer de doeleinden voor de verwerking, de toepasselijke grondslag onder de AVG, een beschrijving van de betrokkenen, een beschrijving van de persoonsgegevens, de toepasselijke bewaartermijnen en de ontvangers waarmee persoonsgegevens worden gedeeld.

Het verwerkingsregister vindt plaats in YSN en wordt beheerd door het AVG-kernteam.

6.1.1 Legitiem doel en doelbinding

Persoonsgegevens worden alleen verwerkt als een specifiek, vooraf bepaald doel is vastgesteld door Stichting el Amal. Dit doel moet duidelijk en in begrijpelijke taal aan de betrokkenen worden uitgelegd. Persoonsgegevens mogen niet voor andere doeleinden worden gebruikt.

Stichting el Amal verwerkt persoonsgegevens om haar verplichtingen als onderwijsinstelling na te kunnen komen. Het schoolbestuur verwerkt persoonsgegevens in de eerste plaats om onderwijs te kunnen bieden aan haar leerlingen en om activiteiten die hieraan ondersteunend zijn te kunnen uitvoeren. Hierbij valt te denken aan verwerkingen in het kader van het aanmeldproces, om te communiceren met leerlingen en ouders/verzorgers, het bijhouden van de leerlingenadministratie, het maken van roosters en om de voortgang bij te houden. Ook verwerkt het schoolbestuur persoonsgegevens van haar medewerkers in haar rol als werkgever. Stichting el Amal verwerkt bij deze werkzaamheden verschillende (categorieën) persoonsgegevens, waaronder contactgegevens, naam, geboortedatum en gegevens betreffende de aard en het verloop van het onderwijs. Stichting el Amal verwerkt deze persoonsgegevens op basis van grondslagen uit de AVG, bijvoorbeeld omdat sprake is van een wettelijke taak of verplichting, een gerechtvaardigd belang of op basis van toestemming.

Als gegevens toch voor een ander doel nodig zijn, dan mag dit alleen als dat doel verenigbaar is met het oorspronkelijke doel. Om te bepalen of dit het geval is, moet onder andere worden gekeken naar:

- De relatie tussen het nieuwe en het oorspronkelijke doel.
- De context waarin de gegevens zijn verzameld en de redelijke verwachtingen van de betrokkenen.
- Het soort persoonsgegevens; gevoelige gegevens verdienen extra bescherming.
- De mogelijke gevolgen voor betrokkenen.
- Bescherming van de gegevens, zoals versleuteling of pseudonimiseren.

Voor elke nieuwe verwerking moet Stichting el Amal de rechtmatigheid, zorgvuldigheid en noodzaak opnieuw beoordelen. De specifieke doeleinden worden voorafgaand aan de verwerking bepaald en vermeld in de privacyverklaring om betrokken te informeren. Ook worden de doeleinden opgenomen in het verwerkingsregister. Voordat gegevens voor een ander doel worden gebruikt, vindt overleg plaats met de privacy officer en indien nodig ook met de functionaris gegevensbescherming.

6.1.2 Grondslag

Stichting el Amal moet voor iedere verwerking van persoonsgegevens een geldige reden hebben. De AVG noemt dit een grondslag. Stichting el Amal verwerkt persoonsgegevens alleen op basis van de in de AVG genoemde grondslagen:

- de betrokkene heeft **toestemming** verleend, bijvoorbeeld voor het maken en delen van foto's of video's.
- de verwerking is noodzakelijk voor de **uitvoering van een overeenkomst** waarbij de betrokkene partij is, bijvoorbeeld het verwerken van salaris om de arbeidsovereenkomst met werknemers na te komen.
- de verwerking is noodzakelijk om te voldoen aan een **wettelijke verplichting**, bijvoorbeeld het delen van salarisinformatie met de Belastingdienst voor de uitvoering van de belastingwetgeving.

- de verwerking is noodzakelijk om **de vitale belangen** van de betrokkene te beschermen, bijvoorbeeld bij een levensbedreigende situatie waarbij het noodzakelijk is dat bepaalde gegevens van een leerling acuut aan hulpverleners moeten worden doorgegeven.
- de verwerking is noodzakelijk om uitvoering te geven aan een **taak van algemeen belang**, hierbij gaat het om wettelijk vastgestelde taken en bevoegdheden. Zo heeft Stichting el Amal de wettelijke taak om onderwijs te bieden.
- de verwerking is noodzakelijk voor de behartiging van een **gerechtvaardigd belang** van Stichting el Amal of van een derde. Denk hierbij aan het verwerken van medewerkersgegevens voor het opstellen van managementrapportages ten behoeve van beleidsontwikkeling of het gebruik van bewakingscamera's op het schoolplein.

De toepasselijke grondslag wordt vooraf vastgesteld, bijvoorbeeld middels een DPIA, en benoemd in de privacyverklaring om betrokken te informeren. Ook wordt de toepasselijke grondslag opgenomen in het verwerkingsregister.

6.2 Informatieplicht

Stichting el Amal verwerkt persoonsgegevens op een behoorlijke en transparante manier. Dit is in begrijpelijke taal inzichtelijk voor de betrokkenen. Stichting el Amal informeert leerlingen en medewerkers voorafgaand aan de gegevensverwerking op transparante wijze via een duidelijke privacyverklaring. Deze privacyverklaring wordt gepubliceerd op de website. Daarnaast informeert de school medewerkers en sollicitanten ook via een aparte privacyverklaring. Hiermee zorgt Stichting el Amal ervoor dat betrokkenen weten welke persoonsgegevens worden verwerkt en voor welke doeleinden dit gebeurt. Ook zijn ze op de hoogte van de rechten die ze hebben.

Wordt gebruikt gemaakt van geautomatiseerde besluitvorming of profilering? Dan gelden extra strenge regels, ook op het gebied van transparantie. Dat betekent onder andere dat medewerkers en leerlingen goed moeten worden geïnformeerd over het gebruik hiervan en duidelijk moet worden uitgelegd op basis van welke criteria het besluit tot stand is gekomen. Ook moet de mogelijkheid bestaan een nieuw besluit te nemen waarbij een mens de gegevens beoordeelt. Op die manier beschermen we medewerkers en leerlingen tegen onrechtmatige verwerking.

6.3 Toestemming

Bij het gebruik van toestemming als grondslag gelden een aantal voorwaarden:

- Toestemming moet op een begrijpelijke en toegankelijke manier worden gevraagd, in duidelijke taal en niet verborgen in algemene voorwaarden of lange teksten.
- Toestemming moet vrijwillig worden gegeven en moet ook weer gemakkelijk ingetrokken kunnen worden.
- Stichting el Amal moet kunnen aantonen dat toestemming is verkregen, bijvoorbeeld door logs of ondertekende formulieren.

- Voor kinderen onder de 16 jaar moet een wettelijke vertegenwoordiger toestemming geven. Dit geldt ook voor personen onder curatele, bewind of mentorschap. Stichting el Amal verifieert of deze vertegenwoordiger daadwerkelijk toestemming heeft gegeven.

Leerlingen (of hun wettelijke vertegenwoordigers) worden in bepaalde situaties om toestemming gevraagd. Denk aan de situatie dat Stichting el Amal foto's of video's van leerlingen maakt en publiceert. Dit mag alleen als de school vooraf toestemming heeft verkregen. Omdat een gezagsrelatie bestaat tussen Stichting el Amal en haar leerlingen en medewerkers, moet goed worden beargumenteerd waarom toestemming in specifieke gevallen in vrijheid kan worden gegeven. Stichting el Amal gaat daarom terughoudend om met het gebruik van deze grondslag. Voordat toestemming als grondslag wordt gebruikt, vindt overleg plaats met de privacy officer en indien nodig ook met de functionaris gegevensbescherming.

6.4 Privacy by design en privacy by default

Toelichting

- *Privacy by design houdt in dat je een zo vroeg mogelijk stadium passende technische en organisatorische maatregelen inbouwt om te voldoen aan de regels uit de AVG. Privacy by default houdt in dat instellingen standaard privacyvriendelijk staan ingesteld.*

Privacy by design betekent dat Stichting el Amal bij de ontwikkeling, het ontwerp, de selectie en het gebruik van toepassingen, diensten en producten zo vroeg mogelijk rekening houdt met privacyrisico's en passende waarborgen inbouwt om de privacy van betrokkenen te beschermen. Neemt Stichting el Amal bijvoorbeeld een leerlingvolgsysteem in gebruik? Dan moet in een vroeg stadium al worden nagedacht over passende toegangsbeperkingen. Leraren horen alleen inzicht te krijgen in de noodzakelijke gegevens van hun eigen leerlingen. *Privacy by default* betekent dat de standaardinstellingen van een product, dienst of proces op de meest privacyvriendelijke instelling staan. Maakt Stichting el Amal bijvoorbeeld een profiel aan op sociale media? Dan mag dit profiel niet standaard openbaar zichtbaar zijn. De stichting heeft op dit moment nog geen vastgesteld socialmediabeleid of richtlijnen. Op schoolniveau zijn wel afspraken gemaakt over de omgang met persoonsgegevens. Hierbij wordt altijd vooraf toestemming gevraagd voor het gebruik van persoonsgegevens, zoals foto's, video's of namen, op sociale media of andere communicatiekanalen. Deze werkwijze is in lijn met de verplichtingen uit de Algemene Verordening Gegevensbescherming (AVG), die voorschrijft dat persoonsgegevens alleen mogen worden verwerkt met een geldige grondslag, zoals toestemming

Hiermee zorgt Stichting el Amal ervoor dat zo vroeg mogelijk rekening wordt gehouden met privacybeginselen en op die manier privacyrisico's tijdig worden gemitigeerd.

6.4.1 Dataminimalisatie

Stichting el Amal verzamelt alleen gegevens die noodzakelijk zijn voor het doel dat voorafgaand aan de verwerking is vastgesteld. De verzamelde gegevens dienen toereikend, ter zake dienend en niet

bovenmatig te zijn. Hiermee voorkomt Stichting el Amal dat te veel gegevens worden verwerkt. Bij de aanmelding van een leerling verzamelt Stichting el Amal bijvoorbeeld alleen de informatie die nodig is om de leerling op de juiste manier in te schrijven. Denk aan naam, geboortedatum, adres en contactgegevens van ouders/verzorgers. Extra informatie, zoals het beroep van de ouders, is niet relevant voor de inschrijving en hoort daarom niet te worden verzameld. Daarnaast moet de verwerking van persoonsgegevens op de minst ingrijpende wijze plaatsvinden. Als het beoogde doel op een privacyvriendelijkere manier kan worden bereikt, dan kiest Stichting el Amal hiervoor. Op deze manier voldoet Stichting el Amal eveneens aan de principes van *privacy by design*.

6.5 Bewaartermijnen

Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor zij zijn verzameld. Dit gebeurt in overeenstemming met het bewaar- en vernietigingsbeleid van Stichting el Amal. Na het verlopen van de toepasselijke bewaartermijnen zorgt Stichting el Amal ervoor dat persoonsgegevens tijdig worden vernietigd (of geanonimiseerd). Hierdoor worden persoonsgegevens beter beschermd tegen onnodige verwerking en datalekken. Zo worden bijvoorbeeld overzichten van schoolprestaties en rapporten uiterlijk tot 2 jaar na uitschrijving van een leerling bewaard. Het schooladvies wordt tot uiterlijk 5 jaar na uitschrijving van een leerling bewaard. Hiervoor wordt de module Privicibasis in LVS gebruikt.

6.6 Afhandelen van 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 bij privacy@elamalscholen.nl.

Voorbeelden van datalekken zijn een gestolen laptop, een verloren usb-stick, of een e-mail met persoonsgegevens die naar de verkeerde persoon is verstuurd. Datalekken worden geregistreerd in het interne register voor beveiligingsincidenten en datalekken (YSN). Risicovolle datalekken moeten worden gemeld aan de Autoriteit Persoonsgegevens en ook aan de betrokkenen als het datalek waarschijnlijk een hoog risico voor hen oplevert. De privacy officer beoordeelt of zo'n melding nodig is. Dit gebeurt als het nodig is in samenspraak met de functionaris gegevensbescherming.

6.7 Data Protection Impact Assessment

Voor elke nieuwe verwerking van persoonsgegevens, bijvoorbeeld een nieuw proces, technologie of applicatie, controleert Stichting el Amal of de privacybeginselen uit de AVG worden nageleefd. Bij verwerkingen met een hoog privacyrisico wordt eerst een *Data Protection Impact Assessment* (DPIA) uitgevoerd. Een DPIA brengt in kaart hoe groot de kans is dat de privacy van betrokkenen wordt geschaad, waar de risico's liggen en welke gevolgen dit kan hebben. Op basis van de uitkomsten van de DPIA neemt Stichting el Amal maatregelen om deze risico's te mitigeren.

6.8 Uitwisseling persoonsgegevens

Een verwerker is een partij die in opdracht van Stichting el Amal persoonsgegevens verwerkt, zoals een leverancier van een leerlingadministratiesysteem. Als Stichting el Amal een verwerker inschakelt om persoonsgegevens te verwerken, dan worden privacyafspraken vastgelegd in een verwerkersovereenkomst. Bepaalt Stichting el Amal samen met één of meerdere partijen het doel en middelen voor de verwerking van persoonsgegevens? Dan is sprake van een zogenaamde gezamenlijke verwerkingsverantwoordelijkheid. In dat geval worden ook contractuele afspraken gemaakt rondom de zorgvuldige en veilige verwerking van gegevens.

Persoonsgegevens kunnen ook beschikbaar worden gesteld aan partijen die niet als verwerkers worden aangemerkt, maar als 'derden'. Deze derden verwerken persoonsgegevens niet in opdracht van een verwerkingsverantwoordelijke, maar voor hun eigen doel. Een verwerkersovereenkomst is daarom ook niet nodig, maar er moet wel een grondslag bestaan om de persoonsgegevens te delen. Denk aan de situatie waarin Stichting el Amal gegevens over medewerkers deelt met de Belastingdienst ten behoeve van de loonaangifte. De Belastingdienst verwerkt deze gegevens voor haar eigen wettelijke doeleinden en handelt niet als verwerker.

Gegevensverwerking buiten de EER

Schakelt Stichting el Amal een verwerker in uit een land buiten de Europese Economische Ruimte (EER) dat geen passend beschermingsniveau biedt? Dan gelden aanvullende voorwaarden. Bij een gegevensdeling buiten de EER moeten namelijk (juridische, technische en organisatorische) waarborgen zijn genomen om het beschermingsniveau ook buiten de EER te laten voldoen aan de AVG, zodat de persoonsgegevens voldoende beschermd blijven. Om dit te bereiken is meer nodig dan alleen het sluiten van een verwerkersovereenkomst. In dat geval maakt Stichting el Amal gebruik van de Europese modelcontracten, de zogenaamde 'Standard Contractual Clauses', en neemt Stichting el Amal aanvullende risicogebaseerde beveiligingsmaatregelen. Ook vindt voorafgaand aan de gegevensdeling afstemming plaats met de privacy officer en afdeling informatiebeveiliging om te beoordelen of de getroffen maatregelen voldoende zijn.

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

6.9 Rechten van betrokkenen

Betrokkenen hebben op grond van de AVG recht op controle op de verwerking van hun persoonsgegevens. Een betrokkene kan onder andere gebruikmaken van het recht op inzage, rectificatie, verwijdering en bezwaar. Leerlingen, leraren en andere medewerkers kunnen een verzoek tot uitoefening van deze rechten indienen via: school directie. Ook hebben betrokkenen het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens.

Stichting el Amal draagt er zorg voor dat de informatie over het uitoefenen van deze rechten op een transparante manier is verstrekt aan betrokkenen via een privacyverklaring. Stichting el Amal zal

binnen de wettelijke termijnen, uiterlijk binnen één maand, schriftelijk reageren op het verzoek. In uitzonderlijke situaties kan de reactietermijn worden verlengd, maar dan wordt dit wel binnen een maand gecommuniceerd. Voor AVG-verzoeken geldt een identificatieplicht, zodat de identiteit van de verzoeker kan worden vastgesteld. Hiertoe kan Stichting el Amal om extra informatie verzoeken, maar zal hierbij terughoudend zijn met het verzoeken om een kopie identiteitsbewijs.

7 Verantwoording IBP

7.1 Naleving AVG

Er vindt toezicht plaats door Stichting el Amal op de naleving van de normen uit dit beleid. Van belang is dat kernteam AVG hun verantwoordelijkheid nemen en medewerkers aanspreken in geval van tekortkomingen. Stichting el Amal besteedt in dit verband actief aandacht aan informatiebeveiliging en privacy bij de aanstelling van medewerkers, tijdens functioneringsgesprekken en via bewustwordingscampagnes.

Mocht de naleving van dit beleid ernstig tekortschieten, dan kan Stichting el Amal de betrokken verantwoordelijke medewerkers maatregelen opleggen binnen de kaders van de CAO en toepasselijke wetgeving. Voor toezicht op de naleving van de AVG vervult de functionaris gegevensbescherming (FG) een belangrijke rol. De FG kan bijvoorbeeld informatie verzamelen over gegevensverwerkingen en beoordelen of deze aan de AVG voldoen. Ook kan de FG adviezen en aanbevelingen verschaffen aan Stichting el Amal

7.2 Rapportage

Stichting el Amal heeft de verantwoordelijkheid om het IBP-beleid formeel goed te keuren en te monitoren of het IBP-beleid door de organisatie wordt toegepast. 2 jaarlijks wordt hierover gerapporteerd in jaarverslag.

7.3 Beleidsherziening

Het IBP-beleid wordt door Stichting el Amal eenmaal per 2 jaar getoetst en indien nodig herzien. Bij een substantiële wijziging van het IBP-beleid of in geval van belangrijke ontwikkelingen of veranderingen in wet- en regelgeving, volgt er indien nodig een beleidswijziging.