Informatiebeveiliging en Privacy-beleid (IBP-beleid)
Lorentz Casimir Lyceum

Colofon:
Vastgesteld door de schoolleiding: mei 2024
Ingestemd door MR: 6 juni 2024

Inhoudsopgave

Inleiding 4

1. Inleiding Privacybeleid 5

1.1 Aanleiding 5

1.2 Wat is het doel van de AVG? 5

1.3 Waarom een privacybeleid? 5

1.4 Reikwijdte 5

1.5 Opzet van het beleid 6

1.6 Privacyrisico's 6

2 Kernbegrippen en definities van de AVG 7

3. Juridisch kader 9

3.1 De Algemene Verordening Gegevensbescherming (AVG) 9

3.2 Overige wetgeving 10

3.3 Overig beleid LCL 10

4. Uitgangspunten en normen voor de verwerking van persoonsgegevens 10

4.2 Toepasselijkheid AVG 10

4.3 Categorieën persoonsgegevens 10

4.4 Doelbinding 10

4.5 Doelen van de verwerking van persoonsgegevens 11

4.6 Grondslag verwerking persoonsgegevens 11

4.7 Minimale gegevensverwerking 11

4.8 Juistheid gegevens 11

4.9 Bewaartermijnen 12

4.10 Delen van gegevens met derden 12

4.11 Verwerking buiten de EU/EER 12

4.12 Beveiliging van persoonsgegevens 12

4.13 Privacy by Design en Privacy by Default 13

5. Transparantie 14

5.1 Verantwoordingsplicht 14

5.2 Rechten van de betrokkene 14

5.3 Meldplicht datalekken 15

5.4 Klachten 15

6. Data Protection Impact Assessment (DPIA) 15

6.1 Doel 15

6.2 Uitgangspunten 15
7. Controle en Naleving 16
7.1 Uitgangspunten 16
7.2 Naleving 16
8. Organisatorisch kader 16
8.1 Inleiding 16
8.2 Rollen en verantwoordelijkheden 17
8.2.1 De rector/bestuurder (eindverantwoordelijke) 17
8.2.2 Privacy coördinator 17
8.2.3 De Functionaris Gegevensbescherming (als onafhankelijk toezichthouder) 17
8.2.3 Overige privacy gerelateerde taken 18
9. Inleiding Informatiebeveiligingsbeleid 18
9.1 Visie op informatiebeveiliging 18
9.2 Definitie Informatiebeveiliging 19
9.3 Doelstelling Informatiebeveiliging 19
9.4 Reikwijdte Informatiebeveiliging 19
9.5 Evaluatie en onderhoud Informatiebeveiliging 19
10. Bestuurlijk kader voor informatiebeveiliging 20
10.1 Kernpunten bestuurlijk kader voor informatiebeveiliging 20
11. Organisatie van informatiebeveiliging 21
11.1 Inrichting van informatiebeveiliging 21
11.2 Verantwoordelijkheden 21
12. Beheersing van informatiebeveiliging 22
12.1 Het proces van informatiebeveiliging 22
12.2 Standaard beveiligingsniveau 23
12.3 Afspraken met derden 24
12.4 Compliance 24
12.5 Rapportage en controle 24
Bijlage A: Overzicht Wet- en Regelgeving 25

Inleiding

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT en brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van informatiebeveiliging en privacy 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. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies. Het is daarom belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan.

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de contiuniteit en betrouwbaarheid van de informatievoorziening gegarandeerd kan worden. Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de vereisten van de huidige wet- en regelgeving

Uit het 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: informatiebeveiliging en privacy beleid afgekort tot IBP.

Dit document bestaat uit twee delen. Het eerste deel gaat over het privacybeleid, het tweede deel gaat over informatiebeveiligingsbeleid in onze school.

1. Inleiding Privacybeleid

1.1 Aanleiding

Per 25 mei 2018 is de General Data Protection Regulation (GDPR) van toepassing in alle lidstaten van de Europese Unie. Deze Europese verordening en de Nederlandse versie daarvan, de Algemene Verordening Gegevensbescherming (AVG) en Uitvoeringswet AVG, vervingen daarmee de Wet bescherming persoonsgegevens (Wbp) in Nederland.

1.2 Wat is het doel van de AVG?

De AVG versterkt de positie van de betrokkenen (de mensen van wie gegevens worden verwerkt). Zij hebben nieuwe privacy rechten gekregen en hun bestaande rechten zijn versterkt. Organisaties die persoonsgegevens verwerken, hebben meer verplichtingen gekregen. De nadruk ligt op de verantwoordelijkheid van organisaties om aan te kunnen tonen dat zij zich aan de wet houden (verantwoordingsplicht).

1.3 Waarom een privacybeleid?

Stichting Algemeen Bijzonder Voortgezet Onderwijs Eindhoven, waaronder het Lorentz Casimir Lyceum valt (hierna ook te noemen: 'LCL'), heeft vanuit haar dienstverlenende taken te maken met het verwerken van persoonsgegevens van leerlingen, ouders, derden (w.o. inhuurkrachten), haar eigen medewerkers en bestuurder. Het gaat hierbij voornamelijk om het verzorgen van specifieke onderwijsbehoeften en extra ondersteuning voor leerlingen. Door toenemende samenwerking met (overheids-) partners neemt de ketenverwerking van persoonsgegevens toe. Het is daarom belangrijk inzicht te hebben waar persoonsgegevens zich in de organisatie bevinden en wie verantwoordelijk is voor de verwerking. Ook wanneer een andere organisatie taken voor LCL uitvoert, kan LCL verantwoordelijk zijn dat deze organisatie de privacywet- en regelgeving correct naleeft.

Met het vaststellen van dit privacybeleid wil LCL in control zijn voor wat betreft het omgaan met persoonsgegevens. Naast een goede beveiliging en verantwoord gebruik van persoonsgegevens waarbij wordt voldaan aan wet- en regelgeving, worden privacyrisico's geïnventariseerd en worden passende maatregelen genomen.

In het privacybeleid geeft LCL op organisatorisch en strategisch niveau duidelijkheid over de keuze van inrichting van privacy en waarborgen dat de verwerking op een rechtmatige wijze plaatsvindt. Daarmee voldoet LCL aan de verantwoordingsplicht uit de AVG[1]. Verder draagt het privacybeleid eraan bij dat besluiten op grond van de AVG binnen LCL op een eenduidige manier worden genomen en dat ook de procedures eenduidig zijn. Hiermee wordt zowel intern als extern transparantie betracht. Betrokkenen moeten erop kunnen vertrouwen dat LCL zorgvuldig en veilig met persoonsgegevens omgaat.

1.4 Reikwijdte

Privacy is een breed begrip om het (grond)recht op de persoonlijke levenssfeer van een individu te beschrijven. Daaronder vallen niet alleen persoonsgegevens, maar ook fysieke en sociale aspecten. Dit beleid richt zich in eerste instantie op de informationele privacy omdat de privacywetgeving zich daarop richt. Informationele privacy betekent bescherming van personen in verband met de informatie die over hen bekend is en ten aanzien van hen wordt toegepast.

Het privacybeleid is van toepassing op de hele organisatie, alle taken en processen, objecten, gegevensverzamelingen en onderliggende informatiesystemen waar LCL verantwoordelijk voor is. Bij de invoering van het beleid worden de proceseigenaren, systeemeigenaren en gegevenseigenaren betrokken.

[1] Artikel 5 lid 2 AVG

Vanuit informatiebeveiliging is het belangrijk dat uiteindelijk passende maatregelen zijn genomen om te voldoen aan wet- en regelgeving.

Het beleid heeft betrekking op het verwerken van persoonsgegevens van betrokkenen, dat wil zeggen alle interne en externe relaties van LCL. Onder interne relaties worden in ieder geval verstaan betrokken werknemers, (oud)werknemers, (oud)bestuursleden, en onder externe relaties worden verstaan leerlingen, ouders/wettelijk vertegenwoordigers, leveranciers, gasten, bezoekers, inhuurkrachten, stagiaires etc. Dit beleid is in lijn met de visie en ambitie van LCL en met de Europese en nationale wet- en regelgeving.

1.5 Opzet van het beleid

In het privacybeleid worden de kaders voor het omgaan met persoonsgegevens vastgelegd. Om de naleving van de AVG aan te kunnen tonen, wordt in een register van verwerkingsactiviteiten inzichtelijk gemaakt welke persoonsgegevens (wel/geen bijzondere persoonsgegevens) worden verwerkt, wat de grondslag en het doel is van de verwerking, welke categorieën van betrokkenen, de inhoud van de gegevens, bronnen, de bewaartermijnen, risicoclassificatie, verwerkers, met wie persoonsgegevens worden gedeeld, veiligheidsmaatregelen etc. Het register maakt toezicht op de verwerkingsactiviteiten mogelijk. Het niet hebben van een overzicht van verwerkingen leidt tot een incompleet beeld van de verwerkte categorieën persoonsgegevens en getroffen maatregelen voor de relevante verwerkingen, processen en technische systemen.

Sommige onderwerpen van dit beleid zijn (of worden) verder uitgewerkt in afzonderlijke regelingen (bijv. het protocol Datalekken en -Incidenten met bijbehorend proces voor afhandeling). Daarnaast wordt in dit beleid verwezen naar gedragscodes die door de Autoriteit Persoonsgegevens zijn vastgesteld en waarin de uitvoering van de AVG nader wordt geconcretiseerd. Het privacybeleid is te beschouwen als een levend document, dat regelmatig aangevuld en/of gewijzigd kan worden.

1.6 Privacyrisico's

Het niet voldoen aan de privacywetgeving kan verregaande gevolgen hebben voor zowel betrokkenen als voor LCL. LCL beoogt dergelijke nadelige gevolgen met dit privacybeleid zoveel als mogelijk te beperken dan wel tot een aanvaardbaar niveau te reduceren, om de voortgang van de dienstverlening en de bedrijfsvoering optimaal te kunnen waarborgen.

Verkeerd gebruik, misbruik of verlies van persoonsgegevens kan een behoorlijke impact hebben op zowel iemands zakelijke als privéleven en leiden tot aanzienlijke schade, zowel materieel als immaterieel. Het kan van invloed zijn op iemands reputatie, leiden tot discriminatie, identiteitsfraude, financiële verliezen, verlies van vertrouwelijkheid van gegevens, verlies van bedrijfsgeheimen en verhindering om rechten en/of vrijheden uit te oefenen.

Voor de organisatie kan het niet voldoen aan de privacywetgeving (of zelfs de schijn daarvan) leiden tot negatieve publiciteit en imagoschade. Daarnaast loopt een organisatie de volgende organisatorische risico's:

- Dwangmaatregelen of boetes opgelegd door de toezichthouder wegens het niet naleven van de wetgeving;
- Onjuiste of onvolledige besluiten (bijvoorbeeld onterechte toewijzing of afwijzing van rechten, vergunningen, klachten e.d.;
- Onterechte en ongewenste doorwerking in ketenverwerkingen;
- Schadeclaims door betrokkenen;
- Hogere kosten bij het achteraf nemen van privacy maatregelen;
- Slechtere performance van de dienstverlening als gevolg van slechte datakwaliteit;
- Wantrouwen als gevolg van datalekken.

Voorbeelden van juridische risico's:

- Niet naleven van privacyregelgeving;
- Niet naleven van sectorale regelgeving;
- Niet naleven van mensenrechten.

2 Kernbegrippen en definities van de AVG

Voor een goed begrip van dit beleid is het noodzakelijk om een aantal begrippen nader te omschrijven. Bij de begripsbepaling wordt zoveel mogelijk uitgegaan van de definities opgenomen in de AVG. Hieronder een overzicht van de begrippen en definities.

Autoriteit Persoonsgegevens (AP): De Autoriteit Persoonsgegevens is de toezichthoudende autoriteit, bedoeld in artikel 51, eerste lid van de AVG, die tot taak heeft toe te zien op de naleving van de verordening en op de verwerking van persoonsgegevens overeenkomstig hetgeen is bepaald bij en/of krachtens de AVG en de Uitvoeringswet AVG.

AVG: Algemene Verordening Gegevensbescherming, (EU) 2016/679 goedgekeurd door het Europees parlement, de Europese Raad op 27 april 2016.

Bestand: Elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.

Betrokkene: Een individueel en natuurlijk persoon op wie een persoonsgegeven betrekking heeft. Dit is zowel een natuurlijke persoon als een éénmanszaak.

Bijzondere persoonsgegevens: Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken, genetische gegevens (DNA/RNA) of biometrische gegevens (bijv. foto's) met het oog op de unieke identificatie van een persoon, en gegevens over gezondheid, of iemands seksueel gedrag of seksuele gerichtheid.

Datalek: Een inbreuk op de beveiliging waarbij persoonsgegevens verloren zijn gegaan of onrechtmatig zijn verwerkt. Wanneer de inbreuk op de persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen meldt de verwerkingsverantwoordelijke deze binnen 72 uur nadat hij van de inbreuk kennis heeft genomen aan de AP. Wanneer er sprake is van een hoog risico deelt de verwerkingsverantwoordelijke de betrokkene de inbreuk onverwijld mee en de AP binnen 72 uur.

Dataportabiliteit: Betrokkenen hebben recht op persoonsgegevens die een organisatie van hen heeft. Organisaties moeten op verzoek van betrokkenen de persoonsgegevens verstrekken in een vorm die het voor betrokkenen makkelijk maakt om hun gegevens te hergebruiken en door te geven aan een andere organisatie. Organisaties zijn daarom wettelijk verplicht om de gegevens in een gestructureerd, veelgebruikt en machine leesbaar formaat te verstrekken.

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.

Functionaris gegevensbescherming (FG): Een FG houdt binnen een organisatie toezicht op de toepassing en naleving van de privacywetgeving. De FG heeft daarnaast een adviserende en coördinerende rol en

fungeert als klankbord voor medewerkers als contactpersoon en aanspreekpunt in de richting van de Autoriteit Persoonsgegevens.

Gegevensbeschermingseffectbeoordeling (GEB), of Data Protection Impact Assessment (DPIA): Een toetsmodel in de vorm van vragenlijsten die de privacy risico's van een specifieke verzameling, de (verdere) verwerking en bewaring van persoonsgegevens op systematische wijze identificeert en lokaliseert.

Ontvanger: Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt.

Persoonsgegevens: Alle informatie over een geïdentificeerde of identificeerbare natuurlijk persoon (de betrokkene); 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 één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Privacy by default: Dit houdt in dat er technische en organisatorische maatregelen genomen moeten worden om ervoor te zorgen dat, als standaard (by default), alléén persoonsgegevens verwerkt worden die noodzakelijk zijn voor het bereiken van het specifieke doel.

Privacy by design: Dit houdt in dat al tijdens de ontwikkeling van producten en diensten aandacht wordt besteed aan privacy verhogende maatregelen. Ook wordt er rekening gehouden met dataminimalisatie (dat wil zeggen dat alleen die persoonsgegevens verwerkt worden die noodzakelijk zijn voor het doel van de verwerking).

Privacy incident: Iedere vraag, klacht of melding met betrekking tot de verwerking van persoonsgegevens binnen LCL wordt beschouwd als een privacy incident. De bekendste vorm van een privacy incident is een datalek.

Privacy Enhancing Technologies (PET): Is een verzamelnaam voor een aantal technieken voor privacybescherming die kunnen worden toegepast. Een centraal principe van PET is het verminderen van de herleidbaarheid van persoonsgegevens naar de betrokkene, met anonimisering van gegevens als zwaarste vorm: na anonimisering zijn de gegevens niet meer te herleiden tot de oorspronkelijke gegevens. Een vergelijkbare techniek is pseudonimisering. De AVG definieert pseudonimisering als "het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat aanvullende gegevens worden gebruikt, op voorwaarde dat deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld".

Toestemming van de betrokkene: Toestemming dient te worden gegeven door middel van een duidelijke actieve handeling, bijvoorbeeld een schriftelijke verklaring, ook met elektronische middelen, of een mondelinge verklaring, waaruit blijkt dat de betrokkene vrijelijk, specifiek, geïnformeerd en ondubbelzinnig met de verwerking van zijn persoonsgegevens instemt. Stilzwijgen, het gebruik van reeds aangekruiste vakjes of inactiviteit mag derhalve niet als toestemming gelden. De toestemming moet gelden voor alle verwerkingsactiviteiten die hetzelfde doel of dezelfde doeleinden dienen. Indien de verwerking meerdere doeleinden heeft, moet toestemming voor elk daarvan worden verleend. Indien de betrokkene zijn toestemming moet geven na een verzoek via elektronische middelen, dient dat verzoek duidelijk en beknopt te zijn en niet onnodig storend voor het gebruik van de dienst in kwestie.

Verstrekken van persoonsgegevens: Het bekend maken of ter beschikking stellen van persoonsgegevens.

Verwerking: Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd door geautomatiseerde procedures, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken d.m.v. doorzending, verspreiden of andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens. In feite iedere handeling t.a.v. persoonsgegevens.

Verwerker: Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke gegevens verwerkt. Een voorbeeld is de organisatie die zorgt voor de verwerking van de salarisadministratie, of bedrijven die ondersteunende diensten leveren ten aanzien van personeelsmanagementsystemen, etc.

Verwerkingsverantwoordelijke: Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van de middelen voor de verwerking van LCL persoonsgegevens vaststelt. Wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijk recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen. In het geval van LCL is dit de Rector/Bestuurder. Ondanks gemandateerde taken en bevoegdheden wordt de Rector/Bestuurder aangemerkt als Verwerkingsverantwoordelijke in de zin van de AVG.

Verwerkersovereenkomst: De uitvoering van een verwerking door een verwerker wordt geregeld in een verwerkersovereenkomst, overeenkomstig het bepaalde in artikel 28 AVG. Dat wil zeggen, indien een organisatie persoonsgegevens voor LCL verwerkt, is er een verplichting om naast de bestaande dienstverleningsovereenkomst ook een aparte verwerkersovereenkomst te sluiten. De verwerkersovereenkomst behelst expliciet afspraken met betrekking tot verwerken van persoonsgegevens en ook de procedure rond de meldplicht datalekken.

3. Juridisch kader

3.1 De Algemene Verordening Gegevensbescherming (AVG)

De bescherming van persoonsgegevens is verankerd in de Grondwet, het Europees Verdrag voor de rechten van de Mens (EVRM) en het Internationaal Verdrag inzake burgerrechten en politieke rechten (IVBPR). De regels over hoe om te gaan met dit grondrecht zijn met ingang van 25 mei 2018 vastgelegd in de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG).

De wijzigingen die de AVG met zich meebracht zijn geen principiële wijzigingen ten aanzien van de Wbp. De kernprincipes van doelbinding, dataminimalisatie, kwaliteit van gegevens en rechtmatige verwerking zijn ook neergelegd in de AVG. Wel is er een verschuiving van taken van de externe toezichthouder (Autoriteit Persoonsgegevens) naar de interne toezichthouder (de Functionaris Gegevensbescherming van LCL).

De belangrijkste veranderingen van de AVG voor LCL zijn:

- De verplichting om een privacybeleid op te stellen;
- De verplichte aanstelling van een Functionaris gegevensbescherming;
- Het bijhouden van een register van verwerkingen van persoonsgegevens;
- Versterking en uitbreiding van bestaande rechten van betrokkenen (recht op informatie, inzage, correctie en verzet), het recht om vergeten te worden en het recht op dataportabiliteit;
- Streng toezicht door de Autoriteit Persoonsgegevens;
- Hoge boetes bij het niet naleven van de wet (tot 20 miljoen euro);

- Verantwoordingsplicht: de organisatie moet aantoonbaar in control zijn met de wet. Dat wil zeggen dat de organisatie moet kunnen aantonen welke organisatorische en technische maatregelen er zijn genomen om de persoonsgegevens te beschermen en daarmee de privacy van betrokkenen te borgen;
- Voor risicovolle gegevensverwerkingen is een gegevensbeschermingseffectbeoordeling (GEB), ofwel: Data Protection Impact Assessment (DPIA) verplicht;
- Processen en systemen moeten worden ingericht volgens de principes van privacy by default en privacy by design.

3.2 Overige wetgeving

In diverse bijzondere wetten die ook voor LCL relevant zijn, zijn ook regels met betrekking tot privacy opgenomen. Bijvoorbeeld de Wet Passend Onderwijs, Telecommunicatiewet, de Jeugdwet, de Leerplichtwet en de Wet op het Voortgezet Onderwijs. In deze bijzondere wetgeving kunnen afwijkende en aanvullende eisen staan. Deze wetten dienen in onderlinge samenhang met de AVG te worden bezien.

Door het in kaart brengen van de specifieke verwerkingen van persoonsgegevens, wordt beoordeeld welke bijzondere wetgeving een rol speelt en hoe aan de daarin neergelegde eisen ten aanzien van privacy tegemoet kan worden gekomen. In bijlage A wordt een overzicht gegeven van wet- en regelgeving met betrekking tot privacy die van toepassing is op Samenwerkingsverbanden Passend Onderwijs.

3.3 Overig beleid LCL

Diverse interne beleidsstukken hebben een relatie met dit privacybeleid of zijn hier een nadere uitwerking van. Daar waar in deze stukken wordt verwezen naar een zorgvuldige omgang met persoonsgegevens of bescherming van privacy wordt verondersteld dat dit beleid hieraan ten grondslag ligt.

4. Uitgangspunten en normen voor de verwerking van persoonsgegevens

4.2 Toepasselijkheid AVG

De AVG is van toepassing op *'de geheel of gedeeltelijke geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen'* (artikel 2 AVG).

Dit betekent dat wanneer LCL persoonsgegevens per computer verwerkt, de AVG van toepassing is. Maar de AVG is ook van toepassing in situaties waarin persoonsgegevens handmatig worden verwerkt, en er dus geen geautomatiseerde verwerking aan de orde is. Als er bijvoorbeeld sprake is van geschreven gespreksnotities van ingehuurde externe professionals met leerlingen of derden verzameld in mappen, dan is de AVG ook van toepassing. De AVG is niet alleen van toepassing op de relatie tussen LCL als samenwerkingsverband met scholen en leerlingen, maar ook op de verhouding die LCL als werkgever heeft met zijn werknemers.

4.3 Categorieën persoonsgegevens

LCL verwerkt categorieën persoonsgegevens van betrokkenen zoals leerlingen, ouders, derden (w.o. inleenkrachten), haar eigen medewerkers en bestuurders. Een compleet overzicht van deze categorieën van persoonsgegevens is opgenomen in het Privacyreglement.

4.4 Doelbinding

Persoonsgegevens worden alleen verwerkt daar waar dat strikt noodzakelijk is voor de uitvoering van vooraf duidelijk bepaalde en uitdrukkelijk omschreven gerechtvaardigde doelen op basis van de grondslagen zoals beschreven in de wet.

Doelen zijn voordat de verwerking plaatsvindt concreet en specifiek geformuleerd. Persoonsgegevens worden niet verder verwerkt voor andere doelen die hiermee onverenigbaar zijn. Het omschreven doel vormt een kader waaraan kan worden getoetst of de verwerking van de gegevens noodzakelijk is voor dat doel en/of verenigbaar is met een ander doel.
Indien er sprake is van verdere (secundaire) verwerking van persoonsgegevens (bijv. voor het doel van (wetenschappelijk) onderzoek), dient te worden nagegaan of deze secundaire verwerking verenigbaar is met de doeleinden waarvoor de persoonsgegevens oorspronkelijk verzameld werden. Betrokkenen dienen omtrent deze verdere (secundaire) verwerking van hun persoonsgegevens geïnformeerd te worden.

4.5 Doelen van de verwerking van persoonsgegevens

De verwerking van persoonsgegevens geschiedt ten behoeve van de realisatie van een samenhangend geheel van ondersteuningsvoorzieningen binnen en tussen de scholen in de regio van het samenwerkingsverband opdat leerlingen die extra ondersteuning behoeven een zo passend mogelijke plaats in het onderwijs krijgen.

Een compleet overzicht van de doelen van de verwerking van persoonsgegevens binnen LCL is opgenomen in het Privacyreglement.

4.6 Grondslag verwerking persoonsgegevens

Verwerking van persoonsgegevens gebeurt alleen indien aan een van de onderstaande voorwaarden is voldaan:

a. De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan LCL is opgedragen.
b. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op LCL rust.
c. De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is (bijvoorbeeld de arbeidsovereenkomst) of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen.
d. De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van LCL of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene zwaarder wegen, met name wanneer de betrokkene een kind is. In het kader van deze grondslag zal dus een belangenafweging moeten plaatsvinden.
e. De verwerking is noodzakelijk om de vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen (levensbelang).
f. De betrokkene heeft ondubbelzinnige toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden. D.w.z. toestemming is expliciet, voordat de verwerking plaatsvindt, gevraagd en gecommuniceerd.

4.7 Minimale gegevensverwerking

LCL beperkt de verwerking van persoonsgegevens tot die gegevens die voor het betreffende doel strikt noodzakelijk zijn (dataminimalisatie). De gegevens dienen met het oog op dat doel toereikend, ter zake dienend en niet bovenmatig te zijn.
Verder moet steeds worden gekeken of het doel niet op een minder ingrijpende wijze kan worden bereikt (principes van proportionaliteit en subsidiariteit).

4.8 Juistheid gegevens

LCL onderkent het belang dat voortdurend wordt nagegaan of de persoonsgegevens die LCL van betrokkenen verwerkt juist en actueel zijn. Als blijkt dat de gegevens niet meer correct zijn, worden ze door LCL gewijzigd of verwijderd.

4.9 Bewaartermijnen

Persoonsgegevens mogen niet langer worden bewaard dan nodig is voor het doel van de verwerking, tenzij het langer bewaren van de persoonsgegevens op grond van wet- of regelgeving verplicht is. Hierbij worden de van toepassing zijnde (wettelijke) bewaar- en vernietigingstermijnen in acht genomen.

Voor een verdere specificatie van de bewaar- en vernietigingstermijnen wordt verwezen naar het Bewaartermijnen en vernietigingsprotocol.

Indien van voornoemde bewaartermijnen voor een bepaald dossier wordt afgeweken, zal hiervoor een motivatie worden gegeven bij het betreffende dossier.

4.10 Delen van gegevens met derden

LCL deelt persoonsgegevens niet zomaar met derden. Dat doet LCL wel als de betrokkene daarvoor toestemming heeft gegeven, als LCL daartoe verplicht is op grond van de wet, als dat nodig is voor de uitvoering van een overeenkomst waarbij betrokkene partij is, of als LCL daartoe een gerechtvaardigd belang heeft.

In sommige gevallen deelt LCL persoonsgegevens wel met derden. Deze derde partijen kwalificeren alsdan als verwerker in de zin van de AVG en LCL als verwerkingsverantwoordelijke. Met derde partijen aan wie LCL persoonsgegevens verstrekt en die onder de verantwoordelijkheid van LCL persoonsgegevens verwerken, sluit LCL een schriftelijke overeenkomst, de verwerkersovereenkomst. In deze overeenkomst worden afspraken gemaakt ter bescherming van de persoonsgegevens. Zo zorgt LCL ervoor dat derde partijen voor doelen en onder voorwaarden die LCL met hen heeft afgesproken, persoonsgegevens verwerkt.

Als LCL samenwerkt met ZZP'ers, tijdelijke krachten of partners die geen verwerkers zijn omdat ze onder direct gezag van LCL staan, en het is noodzakelijk om persoonsgegevens uit te wisselen, sluit LCL een geheimhoudingsovereenkomst.[2]

4.11 Verwerking buiten de EU/EER

De persoonsgegevens worden niet getransfereerd en verwerkt naar derde landen (buiten de EU/EER). De verwerkers van LCL zijn afkomstig uit de Europese Unie, of hebben een relevante vestiging in de EU, waardoor ze zich aan de AVG moeten houden. LCL geeft dus géén persoonsgegevens door naar landen waar persoonsgegevens minder goed worden beschermd.

Indien er in afwijking van deze hoofdregel toch sprake is van doorgifte van persoonsgegevens naar derde landen (buiten de EU/EER), dan zal deze doorgifte uitsluitend plaatsvinden als dit derde land voldoende bescherming biedt. Deze bescherming kan worden geboden op basis van een adequaatheidsbesluit, passende waarborgen, bindende bedrijfsvoorschriften (BCR) of specifieke uitzonderingen, zoals beschreven in de AVG.

4.12 Beveiliging van persoonsgegevens

LCL neemt passende technische en organisatorische beveiligingsmaatregelen om te voorkomen dat de persoonsgegevens worden beschadigd, verloren gaan of onrechtmatig worden verwerkt. Deze maatregelen zijn er mede op gericht om niet noodzakelijke verzameling en verdere (niet noodzakelijke) verwerking van persoonsgegevens te voorkomen.

[2] Vanaf schooljaar 2024-2025

Bij de beveiligingsmaatregelen wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van betrokkenen.

Binnen de organisatie van LCL geldt dat personen slechts toegang hebben tot persoonsgegevens voor zover dat daadwerkelijk nodig is. De toegang van medewerkers tot persoonsgegevens is dan ook beperkt tot de gegevens die noodzakelijk zijn voor de goede uitoefening van hun functie en (dus) hun werkzaamheden. Verder wordt slechts toegang verschaft tot de in de administratie en systemen van LCL opgenomen persoonsgegevens aan:

a. De verwerker die van LCL de opdracht heeft gekregen om persoonsgegevens te verwerken, maar alleen voor zover dat noodzakelijk is in het licht van de gemaakte afspraken;
b. Derden voor zover uit de wet voortvloeit dat LCL verplicht is om toegang te geven of sprake is van een (andere) grondslag voor deze verwerking, bijvoorbeeld de vervulling van een taak van algemeen belang.

Een ieder die betrokken is bij de verwerking van persoonsgegevens binnen LCL is verplicht tot geheimhouding van de betreffende persoonsgegevens, en zal deze gegevens slechts verwerken voor zover dat noodzakelijk is voor de uitoefening van de betreffende functie, werkzaamheden of taak.

4.13 Privacy by Design en Privacy by Default

Privacy by design houdt in dat de organisatie al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) aandacht besteedt aan privacy verhogende maatregelen, ook wel privacy enhancing technologies (PET) genoemd. Daarnaast wordt rekening gehouden met dataminimalisatie: het zo min mogelijk verwerken van persoonsgegevens. Dit betekent dat alleen die gegevens die noodzakelijk zijn voor het doel van de verwerking, worden verwerkt. Op deze manier wordt een zorgvuldige en verantwoorde omgang met persoonsgegevens technisch afgedwongen.

Bij LCL wordt al bij het begin van de ontwikkeling van verwerkingsprocessen en/of aanschaf van informatiesystemen en diensten rekening gehouden met privacy (het "Privacy by design" principe). Bij initiatie van projecten met een ICT of data impact, wordt als onderdeel van het project een DPIA (Data Protection Impact Assessment) uitgevoerd. De DPIA is een verplicht instrument om vooraf na te denken over de privacyrisico's van een bepaalde gegevensverwerking. Wanneer er sprake blijkt van privacygegevens in een project, wordt ernaar gestreefd om de risico's zo veel mogelijk te verkleinen. Onder meer door:

a. **Dataminimalisatie:** dit toe te passen bij alle persoonsgegevens. Alleen de benodigde gegevens worden verwerkt;
b. **Functiescheiding:** de gegevens worden beschermd tegen ongeautoriseerd gebruik. Hiermee zijn zowel op applicatie niveau als op dataniveau de gegevens beschermd tegen misbruik en manipulatie;
c. **Bewaartermijn**: de gegevens worden maximaal volgens de bewaartermijn van de wet bewaard. De bewaartermijnen die in het systeem worden gehanteerd hebben een wettelijke grondslag. Zodra de gegevens de bewaartermijn hebben bereikt, worden ze uit het systeem verwijderd;
d. **Verwerkersovereenkomsten**: bij uitbestedingen van activiteiten waar persoonsgegevens mee gemoeid zijn, worden afspraken gemaakt over hoe de gegevens worden beveiligd en opgeslagen om de risico's rond privacy zo klein mogelijk te houden.

5. Transparantie

5.1 Verantwoordingsplicht

De invulling van de verantwoordingsplicht onder de AVG wordt aangetoond door:

a. **Beleid**: het hebben van een geïmplementeerd informatiebeveiligings- en privacybeleid. Het informatiebeveiligingsbeleid van LCL is verbonden met dit privacybeleid. In het informatiebeveiligingsbeleid staan een aantal passages die betrekking hebben op de beveiliging van persoonsgegevens zoals welke principes gehanteerd worden ten aanzien van te verlenen autorisaties;
b. **Verwerkingsregister**: LCL houdt een register bij van alle verwerkingsactiviteiten die door of namens LCL plaatsvinden. In dit register wordt onder meer opgenomen: de categorieën van betrokkenen, de soorten persoonsgegevens en met wie deze gegevens gedeeld worden. Voor betrokkenen moet duidelijk zijn welke persoonsgegevens worden vastgelegd, verwerkt, waarom en door wie. Per verwerking wordt aangegeven wie de verwerkingsverantwoordelijke is, wie beheerder is en (indien van toepassing) wie verwerker is;
c. **Gegevensbeschermingseffectbeoordeling (GEB) of Data Protection Impact Assessment (DPIA)**: wanneer een verwerking van persoonsgegevens waarschijnlijk veel risico's inhoudt voor betrokkenen, moet LCL vooraf beoordelen wat het effect hiervan is op de bescherming van persoonsgegevens. Er moet dus van tevoren worden gekeken wat de risico's zijn en of die ondervangen kunnen worden;
d. **Procedure datalekken**: Er is sprake van een datalek wanneer persoonsgegevens zijn vernietigd of verloren, gewijzigd, verstrekt of toegankelijk gemaakt op een manier die in strijd is met de AVG. Wanneer er sprake is van een datalek, moet LCL, als verwerkingsverantwoordelijke, dit zo spoedig mogelijk melden bij de toezichthouder (de Autoriteit Persoonsgegevens) zo mogelijk binnen 72 uur. Wanneer er grote kans bestaat dat het datalek negatieve gevolgen heeft voor betrokkenen, moeten deze ook worden gewaarschuwd.

5.2 Rechten van de betrokkene

LCL informeert de betrokkene(n) actief over de verwerking van hun persoonsgegevens, is transparant over het verwerken van de persoonsgegevens en verstrekt deze informatie, conform artikel 12 AVG, in een begrijpelijke vorm. Hierin wordt in ieder geval de volgende informatie vermeld:

a. De contactgegevens van LCL;
b. De contactgegevens van de Functionaris voor Gegevensbescherming van LCL;
c. De doeleinden van de gegevensverwerking en de grondslagen voor de verwerking;
d. Een omschrijving van de belangen van LCL indien de verwerking wordt gebaseerd op het gerechtvaardigd belang van LCL;
e. De (categorieën) ontvangers van de persoonsgegevens, zoals verwerkers of derden;
f. In voorkomend geval: of de persoonsgegevens worden verzonden aan landen buiten de Europese Economische Ruimte (EER);
g. Hoe lang de persoonsgegevens zullen worden bewaard;
h. Dat de betrokkene het recht heeft om LCL te verzoeken om inzage, verbetering of verwijdering van persoonsgegevens, en dat hij het recht heeft om te verzoeken om beperking van de verwerking, om bezwaar te maken of om een beroep te doen op het recht van gegevensoverdraagbaarheid;
i. Dat de betrokkene het recht heeft om zijn toestemming in te trekken, als de gegevensverwerking is gebaseerd op toestemming;
j. Dat de betrokkene het recht heeft om een klacht in te dienen bij de Autoriteit Persoonsgegevens;
k. Of de verstrekking van de persoonsgegevens een wettelijke of contractuele verplichting is, dan wel een noodzakelijke voorwaarde is om een overeenkomst te kunnen sluiten, en of de betrokkene verplicht is om de persoonsgegevens te verstrekken en wat de gevolgen zijn indien hij de persoonsgegevens niet verstrekt;

l. Het bestaan van eventuele geautomatiseerde besluitvorming, vergezeld van nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

De rechten van betrokkenen worden vertaald in heldere, laagdrempelige procedures en worden helder gecommuniceerd richting de betrokkenen.

5.3 Meldplicht datalekken

Een ieder die betrokken is bij een verwerking van persoonsgegevens is verplicht om een datalek per ommegaande te melden bij het AVG-team via AVG@lcl.nl, conform het Protocol datalekken en incidenten van LCL. Deze zal alsdan in overleg treden met de FG om de (eventuele) vervolgstappen te bespreken.

5.4 Klachten

Wanneer een betrokkene van mening is dat het doen of nalaten van LCL niet in overeenstemming is met de AVG, dit beleid of (andere) toepasselijke wet- of regelgeving, dan kan een klacht worden ingediend overeenkomstig de binnen LCL geldende klachtenregeling (gebaseerd op het Protocol voor de afhandeling van rechtsverzoeken door betrokkenen. Een betrokkene kan zich eveneens wenden tot de functionaris voor gegevensbescherming van LCL.

Als een klacht naar de mening van betrokkene door LCL niet correct is afgewikkeld, kan hij zich wenden tot de rechter of de Autoriteit Persoonsgegevens https://www.autoriteitpersoonsgegevens.nl/ .

6. Data Protection Impact Assessment (DPIA)

6.1 Doel

Het doel van een Data Protection Impact Assessment (DPIA) is het in beeld brengen van de privacyrisico's t.a.v. nieuwe en te wijzigen verwerkingen, zodat tijdig en efficiënt de juiste maatregelen genomen kunnen worden ten behoeve van de bescherming van de persoonsgegevens, waaronder het voldoen aan de principes van privacy-by-design en privacy-by-default.

6.2 Uitgangspunten

De uitgangspunten die voor (het uitvoeren van) de DPIA gelden, zijn:

a. Het tijdig en zorgvuldig uitvoeren van een DPIA en het treffen van de daaruit voortkomende maatregelen vallen onder de verantwoordelijkheid van de verwerkingsverantwoordelijke;
b. Een DPIA wordt uitgevoerd voor een specifieke verwerking. Indien het niet mogelijk of niet effectief is om de DPIA voor een bepaalde verwerking uit te voeren, wordt de DPIA uitgevoerd voor het ondersteunende systeem;
c. Een DPIA wordt verplicht uitgevoerd voor die verwerkingen binnen LCL waarvoor geldt dat:
    - Ze betrekking hebben op een substantieel deel van een bepaalde categorie Betrokkenen én waarvoor geldt dat er sprake is van ICT-ondersteuning (door middel van een applicatie, Excel, Word, Outlook of anderszins);
    - Er bijzondere persoonsgegevens verwerkt zullen worden in een context waarbij er sprake is of kan zijn van een hoog privacy-risico;
    - Ondersteund zullen worden d.m.v. een technologie, die LCL nog niet eerder heeft gebruikt;
    - Er sprake is van geautomatiseerde scoretoekenning of geautomatiseerde evaluatie of geautomatiseerde besluitvorming met een mogelijk rechtsgevolg zonder menselijke tussenkomst (profiling).
d. Een DPIA wordt uitgevoerd voordat de nieuwe of gewijzigde verwerking daadwerkelijk plaatsvindt;
e. Elke verplichte DPIA wordt minimaal eens per 3 jaar geëvalueerd;

f. Elke DPIA resulteert in:
    - Een beschrijving van de beoogde verwerking en de doelen voor die verwerking;
    - Een oordeel over de noodzakelijkheid en evenredigheid van de verwerking met het oog op het vastgestelde doel;
    - Een oordeel over de risico's voor betrokkenen;
    - De beoogde maatregelen in de zin van specifieke waarborgen, veiligheidsmaatregelen en mechanismen om die risico's weg te nemen of te beperken.
g. Het resultaat van elke verplichte DPIA wordt ter beoordeling van de rechtmatigheid voorgelegd aan de FG, die op zijn beurt een advies uitbrengt aan de verwerkingsverantwoordelijke;
h. Middels een handreiking wordt een deugdelijke uitvoering van de DPIA's gewaarborgd.

7. Controle en Naleving

De uitvoering van beleid en het bereiken van de doelen geformuleerd in dit beleid valt of staat met de controle en naleving.

7.1 Uitgangspunten

Controle en naleving van dit beleid wordt ingebed in de borgingsinstrumenten binnen LCL. Dit betekent dat:

a. De borging van privacy binnen LCL onderdeel is van het kwaliteitskader;
b. Privacy is ingebed in een audit- en beleidsevaluatiecyclus;
c. De cyclus van 'Plan, Do, Check, Act' de gangbare P&C-cyclus volgt;
d. De FG periodiek de stand van zaken rapporteert aan de portefeuillehouder van het rector/bestuurder.

7.2 Naleving

Mocht de naleving op de bescherming van persoonsgegevens tekort schieten, dan kan LCL ervoor kiezen om de betrokken verantwoordelijke medewerkers een sanctie op te leggen, binnen de kaders van de cao-vo en de wettelijke mogelijkheden.

8. Organisatorisch kader

8.1 Inleiding

Het waarborgen van de privacy ligt niet bij één persoon. Een veelheid van personen binnen de organisatie is betrokken om aan de vereisten van de wet- en regelgeving te kunnen voldoen. Het is daarom van belang om binnen de organisatie duidelijk aan te geven wie waarvoor verantwoordelijkheid draagt.

Het doel van een heldere verdeling van taken en bevoegdheden, van middelen en rapportagelijnen is waarborgen dat op de juiste wijze invulling wordt gegeven aan de eisen van het privacybeleid en de AVG. Binnen LCL worden verschillende rollen met bijbehorende taken en verantwoordelijkheden onderkend. Uiteindelijk is het zorgvuldig omgaan met persoonsgegevens een verantwoordelijkheid voor iedereen in de organisatie.

8.2 Rollen en verantwoordelijkheden

8.2.1 De rector/bestuurder (eindverantwoordelijke)

De rector/bestuurder is eindverantwoordelijk voor de rechtmatige, zorgvuldige en transparante verwerking van persoonsgegevens binnen LCL. Dit geldt ook voor de verwerkingen van persoonsgegevens die ter beschikking worden gesteld aan derden of worden gedeeld in samenwerkingsverbanden.

De rector/bestuurder stelt het beleid, de uitvoeringsmaatregelen en de procedures vast op het gebied van verwerkingen van persoonsgegevens met inachtneming van de aanbevelingen van de FG.

De rector/bestuurder bevordert de beschikbaarheid van voldoende middelen om uitvoering van het privacybeleid te waarborgen. Naleving van de privacywetgeving is de uitdrukkelijke verantwoordelijkheid van de rector/bestuurder en niet van de Functionaris Gegevensbescherming.

8.2.2 Privacy coördinator

De privacy coördinator stuurt het privacy team van LCL aan. Hij/zij is de linking pin tussen LCL en de FG. De privacy coördinator is verantwoordelijk voor het melden van datalekken aan de Autoriteit Persoonsgegevens en voor het afhandelen ervan.

8.2.3 De Functionaris Gegevensbescherming (als onafhankelijk toezichthouder)

LCL is verplicht een FG aan te stellen. De FG moet worden betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens en heeft toegang tot alle persoonsgegevens die in de organisatie in omloop zijn en de diverse verwerkingsactiviteiten die daarmee gepaard gaan. LCL ondersteunt de FG bij de uitvoering van de taken die hem zijn toebedeeld volgens de AVG.

De FG heeft in de eerste plaats de rol van intern toezichthouder. Daarnaast heeft de FG een adviserende en coördinerende rol en fungeert als klankbord voor medewerkers als contactpersoon en aanspreekpunt in de richting van de Autoriteit Persoonsgegevens.

De volgende taken zal de FG uitvoeren:

a. Het toezien op naleving van de AVG, en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming;
b. Het toezien op naleving van het beleid van LCL (als verwerkingsverantwoordelijke) of de verwerker(s) met betrekking tot de bescherming van persoonsgegevens;
c. Het toezien op het correct bijhouden van het register van geconstateerde en gemelde datalekken;
d. Toezien op de juistheid en volledigheid op het register van verwerkingsactiviteiten;
e. Begeleiding voorafgaand aan de uitvoering van een Privacy Impact Assessments (DPIA) en toezicht op correcte (wettelijke) uitvoering hiervan;
f. Jaarlijks rapporteren over de stand van zaken;
g. Het adviseren over het melden van datalekken aan de Autoriteit Persoonsgegevens en begeleiding bij de vervolgstappen;
h. Contactpersoon richting Autoriteit Persoonsgegevens indien afstemming of samenwerking nodig is met de toezichthouder.

De FG heeft geen formele sanctiebevoegdheden. Maar LCL ondersteunt de FG met de volgende maatregelen:

a. De FG is bevoegd om ruimtes te betreden, zaken te onderzoeken en inlichtingen en inzage te vragen om zijn wettelijke taken[3] uit te voeren. Hiertoe maakt de FG eigen keuzes, zonder instructie over de uitvoering van zijn werkzaamheden.

[3] De wettelijke taken zijn het informeren en adviseren van het betrokken personeel, toezicht op de naleving van de AVG, advisering m.b.t. GEB's/DPIA's en samenwerking met en contactpersoon voor de AP.

b. De FG is over de uitvoering van zijn taken tot geheimhouding en vertrouwelijkheid gehouden.
c. De FG rapporteert rechtstreeks aan de rector/bestuurder.

8.2.3 Overige privacy gerelateerde taken

Overige privacy gerelateerde taken bij functionarissen zijn:

- **Hoofden stafafdelingen/sectievoorzitters (uitvoeringsverantwoordelijke):**
  De hoofden van stafafdelingen/sectievoorzitters zijn verantwoordelijk voor de verwerkingen en het beheer van persoonsgegevens die plaatsvinden binnen hun afdeling/sectie. De hoofden stafafdelingen/sectievoorzitters zijn medeverantwoordelijk voor het creëren van bewustwording en de naleving van het privacybeleid binnen de werkprocessen van de eigen afdeling.
- **Systeemeigenaar /functioneel beheerder:**
  Iedere systeemeigenaar of functioneel beheerder is verantwoordelijk voor zijn/haar applicatie en bijbehorende ICT-faciliteiten. De systeemeigenaar of functioneel beheerder moet er voor zorgen dat de applicatie blijft beantwoorden aan de eisen van de wet- en regelgeving, waaronder de privacywetgeving.

9. Inleiding Informatiebeveiligingsbeleid

9.1 Visie op informatiebeveiliging

In dit hoofdstuk staan de uitgangspunten van het informatiebeveiligingsbeleid centraal. Overigens moet worden opgemerkt dat het informatiebeveiligingsbeleid een breder doel heeft dan enkel privacy waarborgen. De uitgangspunten en normen voor de verwerking van persoonsgegevens, zoals uitgebreid wordt omschreven bij het onderdeel Privacybeleid, dienen in dit informatiebeveiligingsbeleid geborgd te zijn.

Informatie is één van de voornaamste bedrijfsmiddelen van LCL. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de bedrijfsvoering maar ook leiden tot imagoschade. Ernstige incidenten hebben mogelijk negatieve gevolgen voor klanten (en haar werknemers), eigen medewerkers, partners en de eigen organisatie. Informatieveiligheid is daarom van groot belang. Informatiebeveiliging (IB) is het proces dat dit belang dient.

De komende jaren zet LCL in op het verhogen van informatieveiligheid en verdere professionalisering van de IB-functie in de organisatie. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van LCL en de basis voor het beschermen van rechten van betrokkenen, klanten en partners.[4] Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

Het proces van informatiebeveiliging is primair gericht op bescherming van informatie van LCL, maar is tegelijkertijd een ‘enabler’; het maakt bijvoorbeeld elektronische dienstverlening op verantwoorde wijze mogelijk, evenals nieuwe, innovatieve manieren van werken. De focus is informatie uitwisselen in alle verschijningsvormen, zoals elektronisch, op papier en mondeling. Het gaat niet alleen over bescherming van privacy, maar ook over bescherming van vitale maatschappelijke functies die worden ondersteund met informatie. Het gaat ook niet alleen over ICT: verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid.

[4] Met betrouwbaarheid wordt bedoeld: beschikbaarheid (continuïteit van de bedrijfsvoering), integriteit (juistheid, volledigheid) en vertrouwelijkheid (geautoriseerd gebruik) van gegevens en informatie.

9.2 Definitie Informatiebeveiliging

Informatiebeveiliging richt zich op de bescherming van informatie tegen dreigingen, om een ongestoorde voortgang van bedrijfsactiviteiten te waarborgen en om risico's te minimaliseren.

Informatiebeveiliging wordt door LCL gedefinieerd als het proces van het beschermen van informatie en gerelateerde componenten (zoals geautomatiseerde informatiesystemen, personen en papieren documenten) tegen toevallige of vooropgezette inbreuken van:

- **Beschikbaarheid:** De mate waarin informatie en essentiële diensten op de juiste momenten beschikbaar zijn voor geautoriseerde gebruikers.
- **Integriteit:** De mate waarin de juistheid, actualiteit en volledigheid van informatie en de verwerkingsmethode is gewaarborgd.
- **Vertrouwelijkheid:** De mate waarin gewaarborgd wordt dat informatie alleen toegankelijk is voor degenen die hiervoor geautoriseerd zijn.

9.3 Doelstelling Informatiebeveiliging

Het doel van dit beleid is het vaststellen van de organisatie en het proces van beheersing van informatiebeveiliging binnen LCL. Het beleid schetst de kaders waaraan informatiebeveiliging dient te voldoen en legt daarmee een basis voor betrouwbare informatievoorziening.

9.4 Reikwijdte Informatiebeveiliging

Dit beleid voor informatiebeveiliging geldt voor alle bedrijfs- en ondersteunende processen met betrekking tot informatie en de daarmee gerelateerde bedrijfsmiddelen, zoals data, verwerkende systemen, opslagmedia, medewerkers, materiële ondersteuning, fysieke omgeving en organisatie.
Het informatiebeveiligingsbeleid is van toepassing op alle personen die deze informatie verwerken. De volgende specifieke doelgroepen worden onderscheiden:

- Alle (tijdelijke) medewerkers, stagiaires, vrijwilligers en inhuurkrachten van LCL;
- Ketenpartners van LCL;
- Leveranciers van LCL.

Ook als informatie niet fysiek binnen LCL aanwezig is, of wanneer taken zijn uitbesteed aan derden, is dit beleid van toepassing.

Dit beleid definieert de verplichte beheersmaatregelen voor informatiebeveiliging voor geheel LCL. Het beleid definieert ook de beheersmaatregelen die gelden wanneer LCL met derde partijen informatie uitwisselt.

9.5 Evaluatie en onderhoud Informatiebeveiliging

De ICT-regisseur toetst het beleid jaarlijks. Het Informatiebeveiligingsbeleid wordt minimaal eenmaal in de drie jaar in zijn geheel geëvalueerd en desgewenst bijgesteld. Tussentijdse evaluaties (op deelgebieden) worden geïnitieerd naar aanleiding van incidenten, analyses van incidentregisters of (organisatorische) wijzigingen. Herziening is mede afhankelijk van wijzigingen in wetgeving, onderliggende normen, het beleid en de beheerorganisatie.

10. Bestuurlijk kader voor informatiebeveiliging

10.1 Kernpunten bestuurlijk kader voor informatiebeveiliging

LCL hanteert dit bestuurlijke kader voor de inrichting en verdere uitwerking van informatiebeveiliging. Dit kader wordt gehanteerd voor de verdere uitwerking van het onderhavige beleid, standaarden en procedures. Daarnaast dient het kader als leidraad wanneer er zich vraagstukken voordoen op het gebied van informatiebeveiliging die niet verder zijn uitgewerkt in beleid of standaarden. LCL hanteert het volgende bestuurlijke kader voor informatiebeveiliging:

a. **Verantwoordelijkheid**
   Iedere medewerker is verantwoordelijk en aansprakelijk voor de veiligheid van de informatie die hem of haar is toevertrouwd. Informatiebeveiliging heeft daarnaast een portefeuillehouder binnen het bestuur.
b. **Integraal risicomanagement**
   Informatiebeveiliging wordt vanuit een integrale visie benaderd en waar mogelijk meegenomen als onderwerp in de Management Review.
c. **Effectiviteit**
   Maatregelen zijn wat inspanning en kosten betreft in balans met het te beschermen belang of waarde. Risico's worden beperkt tot een aanvaardbaar niveau. Het aanvaardbare niveau wordt vastgesteld door de eigenaar en daarbij worden de productie eisen in overweging genomen.
d. **Eigenaarschap**
   Alle processen, applicaties en generieke infrastructuur (fysiek en informatie) hebben één formele eigenaar.
e. **Standaardniveau**
   LCL streeft er naar op het standaardniveau (niveau 3) van informatiebeveiliging, conform het Normenkader Informatiebeveiliging funderend onderwijs, te kunnen opereren:https://www.vo-raad.nl/nieuws/publicatie-normenkader-informatiebeveiliging-en-privacy-voor-funderend-onderwijs .
f. **Beveiligingsbewustzijn**
   Beveiligingsbewustzijn leidt op ieder niveau binnen de organisatie tot medewerkers die weten voor welke risico's zij verantwoordelijk zijn en hoe en waarom zij de beheersmaatregelen uit moeten voeren.
g. **Toegang**
   Inzage in informatie wordt toegekend op basis van Need-to-know. Rechten worden toegekend op basis van Need-to-have.
h. **Pas toe of Leg uit**
   Wanneer wordt afgeweken van vastgesteld beleid of standaarden, legt het bevoegd gezag dit vast in een formele verklaring. De verklaring bevat een risico-inschatting van de afwijking en de mogelijke consequenties.
i. **Continue verbeteren**
   Informatiebeveiliging is een continue verbeterproces. Het managementsysteem van informatiebeveiliging geeft invulling aan de *Plan, Do, Check, Act* cyclus, op basis waarvan het proces van informatiebeveiliging wordt geoptimaliseerd.

11. Organisatie van informatiebeveiliging

11.1 Inrichting van informatiebeveiliging

De rector/bestuurder is eindverantwoordelijk voor informatiebeveiliging en delegeert deze verantwoordelijkheid aan de ICT-Regisseur. Informatiebeveiliging is gedelegeerd aan ICT, aan de eigenaren van de applicaties en aan alle medewerkers die met informatie werken. De ICT-Regisseur ondersteunt bij de invoering en bewaking van informatiebeveiliging. Daarnaast ziet de Functionaris Gegevensbescherming toe op bescherming van persoonsgegevens en naleving van de Algemene Verordening Gegevensbescherming (AVG).

11.2 Verantwoordelijkheden

De rector/bestuurder:

a. Benoemt een eindverantwoordelijke voor informatiebeveiliging, die binnen het bestuur eindverantwoordelijk is voor het managen van de informatierisico's binnen LCL, de beheersing daarvan door informatiebeveiliging en de inrichting en werking van de informatiebeveiligingsorganisatie;
b. Stelt het beleid voor informatiebeveiliging vast;
c. Maakt in het kader van de kwaliteits-cyclus afspraken met de schoolleiding over de invoering van het beveiligingsbeleid, de uitvoering en het toezicht;
d. Bepaalt de risicobereidheid en de daarmee samenhangende tolerantiegrenzen voor LCL;
e. Stelt de noodzakelijke middelen beschikbaar;
f. Is verantwoordelijk voor de implementatie van het beleid voor informatiebeveiliging binnen het eigen bedrijfsonderdeel of de eigen afdeling;
g. Beslist over de mogelijke tegenstrijdige belangen tussen informatiebeveiliging, efficiency in de procesuitvoering en de gebruikersvriendelijkheid van informatiesystemen.

De privacy-coördinator:

a. Is verantwoordelijk voor het naleven van de AVG-wetgeving binnen een organisatie en ziet erop toe dat de privacy van de persoonsgegevens in veilige handen zijn.
b. Onderhoudt contacten en communicatie tussen de diverse verantwoordelijken.
c. verantwoordelijk voor het naleven van de AVG-wetgeving binnen een organisatie en ziet erop toe dat de privacy van de persoonsgegevens in veilige handen zijn.
d. Coördineren van privacyactiviteiten en betrekken medewerkers hierbij. Eerste aanspreekpunt voor medewerkers voor vragen of opmerkingen en (potentiele) datalekken.
e. Adviseert in samenspraak met de FG van Lumen Group verwerkingsverantwoordelijke (rector-bestuurder, directie) over IBP.

AVG-team (LCL):

a. Voorbereiden, opstellen en beheren IBP-beleid en van onderliggende processen, richtlijnen en procedures die het IBP beleid ondersteunen;
b. Uitwerken algemeen IBP-beleid naar specifiek beleid op een uniforme manier.
c. Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering van het IBP-beleid te ondersteunen;
d. Organiseren en verrichten van benodigde risicoanalyses en DPIA's en totstandkoming van een AVG planning;
e. De interne afhandeling van informatieverzoeken, recht van correctie en andere rechten van betrokkenen (zie artikel 12-22 van de AVG);
f. Implementeren van privacy- en informatiebeveiligingsmaatregelen samen met andere collega's (multidisciplinair) en bewaken voortgang. Evalueren van het IBP-beleid en de maatregelen.

De ICT-regisseur:

a. Is verantwoordelijk voor het ontwikkelen en onderhouden van het informatiebeveiligingsbeleid en het managementsysteem voor informatiebeveiliging;
b. Adviseert gevraagd en ongevraagd over de informatiebeveiliging binnen de organisatie en heeft hier mandaat voor;
c. Bewaakt de invoering van het beleid, ontwikkelt generieke standaarden en hulpmiddelen en draagt zorg voor de afstemming van informatiebeveiliging binnen LCL;
d. Verzorgt de rapportage over de stand van zaken op het gebied van informatiebeveiliging aan de rector/bestuurder.

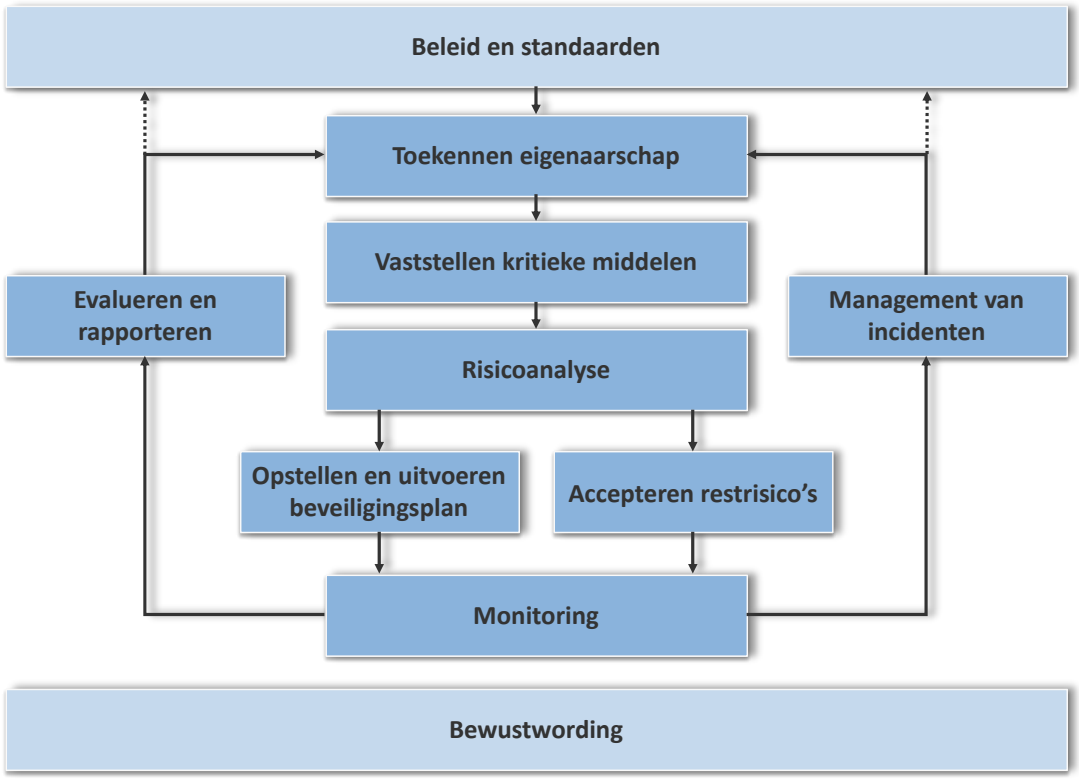
De Functionaris Gegevensbescherming (FG):

a. Houdt toezicht op de bescherming van persoonsgegevens en de naleving van de Algemene Verordening Gegevensbescherming. De FG maakt hierbij mede gebruik van de uitkomsten uit het proces voor informatiebeveiliging.

12. Beheersing van informatiebeveiliging

12.1 Het proces van informatiebeveiliging

LCL hanteert het volgende management raamwerk om informatiebeveiliging te definiëren, te implementeren en te beheersen. Binnen dit raamwerk wijst de rector/bestuurder de toepasselijke verantwoordelijkheden, rollen en taken toe binnen LCL en realiseert een evaluatie en rapportage structuur waarmee de schoolleiding aantoonbaar 'in control' is. LCL definieert het proces van informatiebeveiliging als volgt:



Toelichting:

Beleid en standaarden: Het beleid en onderliggende standaarden beschrijven de kaders waarmee informatiebeveiliging wordt vormgegeven.

Toekennen eigenaarschap: Vaststellen van de eigenaars van processen, applicaties en infrastructuur.

Vaststellen kritieke middelen: Voor elk bedrijfsproces wordt bepaald welke (informatie)middelen kritiek zijn voor het functioneren van het proces. De eigenaar classificeert de informatie die onder zijn/haar verantwoordelijkheid valt, waarbij de gevoeligheid van de informatie wordt vastgesteld. De eigenaar houdt de classificatie up-to-date, gebaseerd op een gestandaardiseerd classificatieschema.

Risicoanalyse: De eigenaar voert een formele en gedocumenteerde risicoanalyse uit om de passende beveiligingsmaatregelen te bepalen en bepaalt eventuele additionele maatregelen, boven op het standaardniveau. Informatiesystemen worden beschermd overeenkomstig de informatie die zij opslaan en verwerken. De beveiligingsmaatregelen zijn zodanig geselecteerd dat een optimale beveiliging wordt verkregen.

Accepteren restrisico's: De mogelijke consequenties van de restrisico's worden beoordeeld en vastgelegd door het management en eventueel vindt aanpassing van het beveiligingsplan plaats.

Opstellen en uitvoeren informatiebeveiligingsplan: Een informatiebeveiligingsplan bevat de resultaten van de stappen van de risicoanalyse en de fasering en aanpak om tot implementatie te komen. De eigenaar van informatie is verantwoordelijk voor de invoering van informatiebeveiligingsmaatregelen. De eigenaar kan de invoering delegeren aan ondersteunende afdelingen.

Monitoring: Maatregelen voor de beveiliging van informatie worden op een dusdanige wijze ingevoerd dat de goede werking van deze maatregelen effectief kan worden gecontroleerd door het management en door een onafhankelijke partij. In het monitoring proces wordt informatie verzameld met het doel om onderliggende risico's te meten en om restrisico's te beoordelen.

Management van incidenten: De afhandeling, rapportage en zo nodig escalatie van informatiebeveiligingsincidenten.

Evalueren en rapporteren: Het functioneren van het proces van informatiebeveiliging wordt beoordeeld. Eigenaren rapporteren de bevindingen aan het management en de Kwaliteitsmanager.

Bewustwording: Beveiligingsbewustzijn leidt op ieder niveau binnen de organisatie tot medewerkers die weten voor welke risico's zij verantwoordelijk zijn en hoe en waarom zij maatregelen uit moeten voeren. Bewustzijn wordt bevorderd door een goede communicatie over dit beleid en de doelstellingen aan de medewerkers. De Kwaliteitsmanager brengt informatieveiligheid planmatig en periodiek onder de aandacht van verschillende doelgroepen binnen de organisatie, om zo het bewustwording vergroten.

12.2 Standaard beveiligingsniveau

De basis voor de inrichting van het informatiebeveiligingsmanagement binnen LCL is dit beleidsdocument, waarvoor ISO 27001/27002 als inspiratie diende. Formele certificering conform ISO 27001 wordt voor LCL niet als noodzakelijk gezien, inrichting van een goede ICT-structuur echter wel – dit beleid is daarvoor de basis. Dit beleidsstuk geeft richting aan de maatregelen. Deze worden genomen op basis van best-practices, waarbij naast de ISO 27002 nu ook het Normenkader Informatiebeveiliging en Privacy VO als uitgangspunt worden genomen.

12.3 Afspraken met derden

De eigenaar van informatie maakt afspraken met derden (bijvoorbeeld afnemers van gevoelige informatie of dienstverleners) over de te treffen beveiligingsmaatregelen (bijvoorbeeld in een verwerkersovereenkomst of Service Level Agreement (SLA)). Het betreft hier dienstafspraken met leveranciers, intern binnen LCL en extern. Afspraken moeten formeel vastgelegd worden over de grenzen heen van organisaties en bedrijfsonderdelen. Dit beleid is het uitgangspunt voor de informatiebeveiligingsaspecten van deze afspraken. De schoolleiding is verantwoordelijk voor het nakomen van de afspraken door de leverancier.

12.4 Compliance

LCL voldoet controleerbaar aan alle relevante wet- en regelgeving die zijn gerelateerd aan informatiebeveiliging, aan contractuele verplichtingen en beleid, inclusief nationale en internationale standaarden die het functioneren van LCL activiteiten betreffen.

12.5 Rapportage en controle

De schoolleiding rapporteert periodiek over de status van informatiebeveiliging. De ICT-regisseur combineert deze voortgangsrapportages met zijn eigen bevindingen en rapporteert over het geheel aan de rector/bestuurder. Periodiek vindt er interne controle plaats op de informatiebeveiligingsmaatregelen van zowel de infrastructuur als van kritische informatiesystemen.

Bijlage A: Overzicht Wet- en Regelgeving

Hieronder een overzicht van wet- en regelgeving en richtlijnen met een privacy component die van toepassing is op Samenwerkingsverbanden Passend Onderwijs.

a. Internationaal/Europees

- Artikel 17 van het VN-verdrag voor Burgerlijke en Politieke rechten;
- Artikel 8 van het Europees Verdrag voor de Rechten van de Mens;
- Artikel 7 Handvest grondrechten van de Europese Unie;
- Algemene Verordening Gegevensbescherming (AVG) / General Data Protection Regulation (GDPR);
- Richtlijn Netwerk en informatiebeveiliging (NIB);
- Richtlijn gegevensbescherming politie en justitie;
- eIDAS - Europese Verordening e-identity en vertrouwensdiensten;
- e-Privacyrichtlijn (wetgeving met betrekking tot o.a. cookies).

b. Landelijk

- Uitvoeringswet AVG;
- Artikelen 10 tot en met 13 van de Nederlandse Grondwet;
- Algemene wet bestuursrecht (hoofdstuk 5);
- Jaarrekeningrecht: Jaarverslag: verantwoording privacybeleid en security;
- Telecommunicatiewet (hoofdstuk 11);
- Wet op de ondernemingsraad (instemmingsrecht);
- Auteurswet;
- Jeugdwet;
- Wet op de Loonbelasting;
- Leerplichtwet;
- Wet op het Primair Onderwijs;
- Wet op het Voortgezet Onderwijs;
- Wet op de Expertisecentra.

c. Beleid Autoriteit Persoonsgegevens

De AP heeft diverse richtlijnen gepubliceerd, waaronder:

- Richtsnoeren beveiliging van persoonsgegevens;
- Beleidsregels Meldplicht datalekken;
- Richtlijnen actieve openbaarmaking persoonsgegevens;
- Richtlijnen publicatie persoonsgegevens op internet;
- Richtlijnen recht op dataportabiliteit;
- Richtlijnen voor functionarissen voor de gegevensbescherming;
- Richtlijnen De zieke werknemer;
- Richtlijnen kopie identiteitsbewijs.