Bachelor Scriptie

Één jaar na de invoering van de AVG:

Onderzoek naar Algemene Verordening Gegevensbescherming binnen Stichting Lucas Onderwijs

Arradi Moustach – 20057860 **19 september 2019**

De Haagse Hogeschool

Faculteit Business, Finance & Marketing

Bachelor Scriptie Finance & Control

Docentbegeleider: **mr. R. Aydogdu**

Opdrachtgever: **drs. H.J. Postema**

Bedrijfsbegeleider: **Stichting Lucas onderwijs**

Één jaar na de invoering van de AVG:

Onderzoek naar Algemene Verordening Gegevensbescherming binnen Stichting Lucas Onderwijs

Datum: **19 september 2019**

Auteur: **A. Moustach**
Studentnummer: **20057860**

Opdrachtgever: **Stichting Lucas onderwijs**
Bedrijfsbegeleider: **drs. H.J. Postema**

Onderwijsinstelling: **De Haagse Hogeschool**
Opleiding: **Finance & Control**
Docentbegeleider: **mr. R. Aydogdu**

Vrijgave door bedrijfsbegeleider
Naam : H.J. Postema
Handtekening :……
Datum :……

Voorwoord

Voor u ligt de afstudeeropdracht “Één jaar na de invoering van de AVG: Onderzoek naar Algemene Verordening Gegevensbescherming binnen Stichting Lucas Onderwijs”. Deze heb ik geschreven in opdracht van Stichting Lucas Onderwijs waar ik werkzaam ben. Dit is ter afsluiting van mijn deeltijdstudie Finance & Control die ik heb gevolgd aan de Haagse Hogeschool. Dit onderzoek heb ik uitgevoerd in opdracht van de heer H.J.M. Postema, manager van de afdeling Financiën & Administratie. De heer Postema wilde een adviesrapport waarin inzichtelijk wordt gemaakt of de organisatie AVG-compliant is ten aanzien van personeelsgegevens, en welke eventuele verbeteringen kunnen worden toegepast om AVG-compliant te zijn.

Ik ben in april 2019 begonnen met deze afstudeeropdracht. Tijdens de opdracht was het lastig om balans te vinden tussen werk, studie en gezin. Dit heeft tot vertraging geleid. De afstudeeropdracht was voor mij een enorme uitdaging. Er was veel inzet en doorzettingsvermogen nodig om dit te kunnen realiseren.

Tijdens de opleiding heb ik veel geleerd. Het was een boeiende en leerzame ervaring. Het contact met docenten heb ik als zeer positief ervaren. De opleiding heeft bijgedragen aan mijn persoonlijke ontwikkeling als financieel adviseur.

Ik wil een aantal mensen bedanken voor hun hulp en steun. In het bijzonder mijn studiebegeleider de heer R. Aydogdu, mijn broer Y. Moustach en de Security Officer Lucas Onderwijs de heer F. Bos. Zij hebben mij op hun eigen manier terzijde gestaan.

Arradi Moustach

Den Haag, 30 juli 2019

Management Samenvatting

Lucas Onderwijs is een schoolbestuur in Zuid-Holland. Momenteel vallen zevenenveertig scholen voor basisonderwijs, vier scholen voor speciaal basisonderwijs, drie expertisecentra en drie regio's voor voortgezet onderwijs met in totaal zesentwintig vestigingen onder Lucas Onderwijs. Lucas Onderwijs heeft ongeveer 4.000 medewerkers in dienst en heeft een leerlingaantal van 34.000.

Lucas Onderwijs wil zich aan de wet houden en wil haar medewerkers het vertrouwen geven dat zij zorgvuldig met hun gegevens omgaat. Dit onderzoek gaat over de vraag of de organisatie de Algemene Verordening Gegevensbescherming juist heeft geïmplementeerd. In het adviesrapport moet naar voren komen welke veranderingen in de bedrijfsvoeringen doorgevoerd moeten worden om AVG-compliant te zijn. Vanwege de grote hoeveelheden gegevensverwerkingen in de organisatie en het tijdsbestek waarin dit onderzoek moest plaatsvinden is afgesproken om het onderzoek uit te voeren op personeelsgegevens. De onderzoeksvraag hiervoor luidt: Wat moet er veranderen aan de huidige bedrijfsvoering van Lucas Onderwijs om te voldoen aan de AVG-richtlijn ten aanzien van de vaststelling en verwerking van personeelsgegevens?

Voor dit onderzoek is de Wet Bescherming Persoonsgegevens onderzocht. Deze is per 25 mei 2018 komen te vervallen. Vervolgens is de nieuwe verordening die per 25 mei 2018 in werking is getreden onderzocht. Deze wetten vormen samen het theoretische kader van het onderzoek. Aan de hand van een casestudy is documentenonderzoek gedaan en zijn interviews afgenomen om de huidige situatie van de organisatie te beschrijven. De huidige werkwijze is met de Algemene Verordening Gegevensbescherming vergeleken en hieraan getoetst.

De Wet Bescherming Persoonsgegevens is een uitwerking van de Europese Data Protectie Richtlijn. Deze is ingegaan op 1 september 2001 en verving de toen geldende Wet Persoonsregistratie die zijn oorsprong vindt in artikel 10 van de grondwet. Deze Richtlijn was bedoeld om de verschillen tussen de nationale wettelijke regelingen in de Europese Unie inzake gegevensbescherming te harmoniseren. De Richtlijn sloot beter aan op de ontwikkelingen op het gebied van ICT. De Algemene Verordening Gegevensbescherming is een Europese verordening en heeft automatisch directe werking op iedere lidstaat. De Algemene Verordening Gegevensbescherming is bindend en moet letterlijk door alle lidstaten op dezelfde manier worden uitgevoerd. De Algemene Verordening Gegevensbescherming biedt beperkte mogelijkheden om wetgeving aan te passen. Het doel van de Algemene Verordening Gegevensbescherming is om de grondrechten en de fundamentele vrijheden van natuurlijke personen te beschermen en om het vrije verkeer van gegevens binnen de Europese interne markt te beschermen en te waarborgen. Met de invoering van de Algemene Verordening Gegevensbescherming hebben betrokkenen nieuwe privacy-rechten gekregen en werden de bestaande rechten versterkt. Verantwoordelijken die persoonsgegevens verwerken krijgen daarentegen meer verplichtingen.

De Algemene Verordening Gegevensbescherming is strenger in de uitvoering dan de vorige privacywet. De Algemene Verordening Gegevensbescherming verplicht in een aantal gevallen om een Functionaris voor de Gegevensbescherming aan te stellen. Deze moet worden aangemeld bij de Autoriteit Persoonsgegevens. De Functionaris voor de Gegevensbescherming heeft een autonome positie ten aanzien van zijn taken. De organisatie dient een dataregister bij te houden van de verwerking van persoonsgegevens en incidenten van datalekken. Datalekken dienen in sommige gevallen te worden gemeld bij de Autoriteit Persoonsgegevens. Het niet melden van datalekken staan forse sancties op ten opzichte van de Wet Bescherming Persoonsgegevens. Bij een nieuwe vorm van gegevensverwerking is het uitvoeren van een Data Protection Impact Assessment verplicht. De Algemene Verordening Gegevensbescherming kent zes beginselen die organisaties in ogenschouw moeten houden. Een gegevensverwerking moet rechtmatig zijn en de betrokkenen moeten op de hoogte zijn wat er met hun gegevens gebeurd. Er mogen niet meer gegevens worden verwerkt dan nodig is. Persoonsgegevens dienen te worden beveiligd tegen ongeoorloofd toegang of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. De rechten van betrokkenen zijn in de nieuwe

privacywet versterkt. Zij hebben het recht om hun gegevens in te zien en correctie indien zij van mening zijn dat de gegevens onjuist zijn. Zij kunnen eisen dat de gegevensverwerking wordt gestaakt of beperkt. Zij kunnen vragen om hun gegevens te wissen. Zij hebben tevens het recht om persoonsgegevens te ontvangen of om de gegevens over te dragen aan een andere organisatie met dezelfde soort dienst.

Uit het onderzoek is gebleken dat Lucas Onderwijs op de bekeken gebieden AVG-Compliant is. Zij voldoen aan de harde eisen, maar er zijn ook enkele onbewuste tekortkomingen die tegenstrijdig zijn met de verordening. De organisatie is zich bewust van de inhoud van de verordening en zijn er noodzakelijke aanpassingen gedaan die vanuit de verordening worden geëist. De organisatie heeft haar medewerkers bewust gemaakt van de nieuwe privacywetgeving door middel van bijeenkomsten en nieuwsbrieven. De formele zaken zijn in lijn met de verordening gebracht. Er is een Functionaris voor de Gegevensbescherming benoemd en aangemeld bij de Autoriteit Persoonsgegevens. Daarnaast heeft de organisatie gekozen om een Security Officer in te zetten wat niet vanuit de verordening wordt verplicht. Er is een privacyverklaring opgesteld en er zijn verwerkersovereenkomsten afgesloten met de verwerkers. De organisatie heeft technische en organisatorische maatregelen getroffen om persoonsgegevens te beschermen.

Op basis van de conclusie zijn een aantal aanbevelingen geformuleerd. Wanneer deze aanbevelingen zijn opgevolgd kan gesteld worden dat Lucas onderwijs een jaar na de invoering van de verordening in de organisatie voldoet aan de verordening. Medewerkers wordt niet gevraagd om toestemming voor de gegevensverwerking en zij worden ook niet gewezen op hun rechten. Volgens de verordening is dit een vereiste. De personeelsdossiers zijn niet compleet en voldoet hiermee niet aan het juistheidbeginsel. Alle documenten dienen te worden opgenomen in het de personeelsdossiers en de medewerkers dienen hierover geïnformeerd te worden. In de rapportagetool Capisci worden persoonsgegevens van medewerkers verwerkt en zijn hier niet over geïnformeerd. De gegevens zijn verzameld voor een ander doel en voldoen bovendien niet aan het beginsel van minimale gegevensverwerking. Dit kan worden opgelost door de namen van medewerkers te vervangen door personeelsnummers. Met de financiële afdeling worden te veel persoonsgegevens gedeeld voor het registreren van personele voorzieningen. Er dient in de organisatie te worden afgestemd welke gegevens noodzakelijk zijn om personele voorzieningen te registreren in de boekhouding. Een van de belangrijkste aandachtspunten voor de organisatie is de bewaartermijn van persoonsgegevens. Dit is in de huidige situatie niet goed georganiseerd. Het verdient aanbeveling om aanpassingen in systemen door te voeren die een bewaartermijn classificatie mogelijk maken. Daarnaast dienen de bewaartermijnen bepaald te worden en moeten deze binnen de organisatie worden gecommuniceerd. De organisatie dient tevens regels op te stellen ten aanzien van de opslag van persoonsgegevens. Hierbij moet aangestuurd worden om persoonsgegevens niet langer meer via de e-mail te versturen en dienen deze niet meer lokaal te worden opgeslagen. De organisatie doet er goed aan om gebruik te maken van het Document Management Systeem, zodat toegezien kan worden op de bewaartermijn van persoonsgegevens. Voor de Security Officer wordt aanbevolen hem te positioneren onder de directeur van het stichtingsbureau. Dit biedt bescherming ten aanzien van zijn andere taken van informatiebeheer. Ten slotte ontbreekt het recht van dataportabiliteit in de privacyverklaring. Dit is een recht van medewerkers en dient in de verklaring te worden opgenomen.

Lijst van afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BRP	Wet basisregistratie personen
CvB	College van Bestuur
DMS	Document Management Systeem
DPIA	Data Protection Impact Assessment
EU	Europese Unie
EDPR	Europese Data Protectie Richtlijn
FG	Functionaris Gegevensbescherming
IAM	Identity Acces Management
IT	Informatie Technologie
ICT	informatie- en communicatietechnologie
UWV	Uitvoeringsinstituut werknemersverzekeringen
WBP	Wet Bescherming Persoonsgegevens

Inhoudsopgave

1. Inleiding

Dit adviesrapport begint met een beschrijving van Lucas Onderwijs met haar missie, visie en organisatiestructuur. Vervolgens worden de aanleiding en probleemstelling van het onderzoek beschreven met de centrale hoofdvraag en deelvragen. Ten slotte komt de methode van het onderzoek aan bod om de aanpak van het onderzoek te beschrijven en wordt de opbouw van het adviesrapport weergegeven in de leeswijzer.

1.1 De Organisatie

Lucas Onderwijs profileert zich als een dynamisch en betrokken onderwijsbestuur. Onder het bestuur van de stichting vallen in het primair onderwijs 46 basisscholen, 4 scholen voor speciaal basisonderwijs en 3 expertisecentra in de gemeenten Den Haag, Leidschendam-Voorburg, Pijnacker-Nootdorp en Rijswijk. In het voortgezet onderwijs heeft Lucas Onderwijs 25 locaties in de regio's Den Haag, Leidschendam-Voorburg, Delft, Rijswijk, Pijnacker-Nootdorp en Westland. Op de scholen zijn ruim 4.000 personeelsleden werkzaam die de zorg hebben voor meer dan 34.000 leerlingen.

1.2 Visie en missie

Lucas Onderwijs en iedereen die aan Lucas Onderwijs is verbonden, werkt vanuit de missie, de visie en de waarden zoals verwoord in De Grondslag Verdiept. Deze beginselverklaring omvat vijf kernwaarden: respect, naastenliefde, genade, ontwikkeling en bezieling. Samen met de statuten van de stichting Lucas Onderwijs vormt dit het fundament waarop Lucas Onderwijs in gezamenlijkheid onderwijs en (de onderdelen van) de organisatie baseren. Lucas Onderwijs stelt zijn scholen in staat en stimuleert hen het best denkbare onderwijs te bieden, opdat iedere leerling zich kan ontwikkelen tot een zelfbewuste, verantwoordelijke en kansrijke burger. Lucas Onderwijs geeft dat vorm door samen te werken:

- Vanuit waarden, in oorsprong ontleend aan de traditie van de christelijke geloofsgemeenschap met universele geldigheid voor een humane samenleving;
- Aan aantrekkelijk onderwijs, dat zich onderscheidt door ontwikkeling, aandacht voor kwaliteit, goede zorg voor de medewerkers en solidariteit met kansarmen;
- In actief partnerschap met de maatschappelijke omgeving;
- Met ruimte voor diversiteit van de scholen.

Bij het bieden van het best denkbare onderwijs kijkt Lucas Onderwijs naar de jeugd van 0 tot en met 20 jaar en de wereld waarin deze groep zich ontwikkelt. De verbinding tussen school, thuis en de (leef)omgeving van leerlingen is van essentieel belang om leerlingen zich te kunnen laten ontwikkelen tot zelfbewuste, verantwoordelijke en kansrijke burgers die zich gewetensvol inzetten voor het algemeen belang naast het eigen belang. Het Verdrag inzake de Rechten van het Kind bevat voor het werk van Lucas Onderwijs de minimale basis van respect voor en vertrouwen in en van het kind.

1.3 De organisatiestructuur

De scholen in het primair onderwijs zijn samengevoegd in 4 clusters. De clusterdirecteuren sturen de clusters aan en vormen de schakel naar het College van Bestuur via het bestuur managementteam primair onderwijs. In het voortgezet onderwijs zijn de scholen gebundeld tot instellingen. De instellingsdirecteuren nemen deel aan het bestuur managementteam voortgezet onderwijs dat het College van Bestuur ondersteunt.

Lucas Onderwijs kent op centraal niveau een stichtingsbureau. De stichting wordt geleid door een tweehoofdig bestuur, onder leiding van de Raad van Toezicht. Het stichtingsbureau heeft vijf stafdiensten die de scholen en het College van Bestuur ondersteunen. Deze stafdiensten zijn Onderwijs, Kwaliteit en Innovatie, Human Recource, Financiën & Administratie, Informatiebeheer en Facilitaire Zaken. In Bijlage 1 is het organogram van de stichting te vinden.

1.4 Aanleiding

Dagelijks vinden er grote hoeveelheden gegevensverwerkingen plaats. Deze verwerkingen worden voor verschillende doeleinden gebruikt. Iedereen moet ervan uit kunnen gaan dat er altijd zorgvuldig met zijn of haar persoonsgegevens wordt omgegaan. Dat is niet altijd vanzelfsprekend. In het nieuws verschijnen regelmatig nieuwsberichten over datalekken. Een recent voorbeeld hiervan is een artikel van de Telegraaf over een datalek wat zich heeft voorgedaan bij het Haga ziekenhuis in Den Haag, waarbij 85 medewerkers een patiëntendossier van een realityster hebben ingezien zonder dat zij betrokken waren bij de behandeling van de patiënt. Het Haga ziekenhuis heeft een voorlopige boete van 460.000 euro gekregen vanwege de slechte interne beveiliging van patiëntendossiers (Schoolenberg, 2019). Het is de eerste boete die de Autoriteit Persoonsgegevens (hierna: AP) uitdeelt op basis van de privacywetgeving Algemene Verordening Gegevensbescherming (hierna: AVG).

Met het gegeven voorbeeld hierboven blijkt dat één jaar na de invoering van de AVG de organisatie niet AVG-compliant is. Het toezien op de naleving van de AVG is een continu proces en moet dit gewaarbord zijn. Het doel van het onderzoek is om te onderzoeken of Lucas onderwijs de AVG juist heeft geïmplementeerd en of zij een jaar na de implementatie wel voldoen aan deze privacy-verordening. Dit onderzoek beperkt zich tot de verwerking van personeelsgegevens vanwege de omvang en de tijd die hiervoor beschikbaar is.

Ten aanzien van de personeelsgegevens verwerkt Lucas onderwijs persoonsgegevens op grond van een arbeidsrelatie die de verwerking van de gegevens noodzakelijk maakt. De verwerking is tevens noodzakelijk om te kunnen voldoen aan wettelijke verplichtingen zoals de plicht om aangifte te doen bij de belastingdienst en afdrachten aan het pensioenfonds. De grondslag voor de verwerking van leerling gegevens vindt haar grondslag in de Wet op het Primair onderwijs en de Wet op het voortgezet onderwijs.

1.5 Probleemomschrijving

De AVG-richtlijn dwingt organisaties na te denken over hoe organisaties persoonsgegevens verwerkt en beschermt. Lucas Onderwijs heeft de verantwoordelijkheid om aan te tonen dat zij voldoet aan de AVG-richtlijn ten aanzien van de verwerking van persoonsgegevens aan haar medewerkers. Daarnaast is Lucas onderwijs verplicht deze verantwoording af te leggen aan de AP indien deze daar om vraagt.

Lucas onderwijs verwerkt jaarlijks persoonsgegevens van ongeveer 4.000 medewerkers.
De verwerking van deze gegevens gebeurt zowel binnen de organisatie als door derden. Binnen de organisatie kan je bijvoorbeeld denken aan de aanstelling en ontslag, functioneringsgesprekken en (ziekte)verzuim van medewerkers. Daarnaast vindt gegevensuitwisseling plaats met pensioenfonds, belastingdienst en UWV. Lucas onderwijs vindt het belangrijk dat al deze processen voldoen aan privacywetgeving en dat haar medewerkers vertrouwen hebben in de verwerking van hun gegevens.

Dit onderzoek is erop gericht om te onderzoeken in hoeverre Lucas onderwijs voldoet aan privacywetgeving met betrekking tot de processen van gegevensverwerking van haar medewerkers. De processen dienen te worden beschreven en worden onderzocht of voldaan wordt aan de AVG-richtlijn. De uitkomst van het onderzoek moet leiden tot een advies van eventueel te nemen maatregelen om AVG-compliant te zijn. De centrale onderzoeksvraag voor dit onderzoek luidt: *“Wat moet er veranderen aan de huidige bedrijfsvoering van Lucas Onderwijs om te voldoen aan de AVG-richtlijn ten aanzien van de vaststelling en verwerking van personeelsgegevens?”*

1.6 Deelvragen

Om tot een antwoord te komen op de centrale onderzoeksvraag dienen onderstaande deelvragen te worden beantwoord.

1. Wat houdt de Algemene Verordening Gegevensbescherming in?
2. Waar moet een organisatie aan voldoen om AVG-Compliant te zijn?
3. Wat is de huidige werkwijze van Lucas onderwijs ten aanzien van de verwerking van persoonsgegevens?
4. Voldoet de huidige werkwijze aan de AVG-richtlijn?

1.7 Methode van onderzoek

Bij aanvang van het onderzoek is gestart met een literatuuronderzoek om informatie in te winnen op het gebied van AVG. Om antwoord te kunnen geven op de eerste deelvraag “Wat houdt de Algemene Verordening Gegevensbescherming in?” is het onderwerp ingeleid door eerst kort onderzoek gedaan naar de voorganger van de AVG, de Wet Bescherming Persoonsgegevens. Dit is hierin opgenomen om verschillen met de AVG te benadrukken. Hierna is er door middel van de verordening van de AVG en literatuuronderzoek gedaan naar de AVG. De AVG is eerst bestudeerd op het gebied van organisatie en wijzigingen t.o.v. de Wbp. Hierna zijn de belangrijke eisen en verplichtingen uitgelicht om antwoord te geven op de tweede deelvraag “Waar moet een organisatie aan voldoen om AVG-Compliant te zijn?”. Hierbij werden de beginselen, de privacyrechten, datalekken en het gebruik van de Data Protection Impact Assessment behandeld. Ook is er onderzoek gedaan naar een stappenplan van de AVG dat voor organisaties is opgezet om te helpen voorbereiden op de AVG. Het stappenplan is opgenomen in het literatuuronderzoek omdat dit nuttig is bij het beoordelen of Lucas Onderwijs de AVG correct heeft geimplementeerd en of Lucas Onderwijs AVG-Compliant is.

In hoofdstuk 3 moest antwoord worden gegeven op deelvraag 3 “Wat is de huidige werkwijze van Lucas onderwijs ten aanzien van de verwerking van persoonsgegevens?” En deelvraag 4 “Voldoet de huidige werkwijze aan de AVG-richtlijn?” Dit hoofdstuk is onderdeel van een praktisch onderzoek bij Lucas Onderwijs. Met behulp van het literatuuronderzoek is er een praktische onderzoeksmethode opgesteld waar onderzoek gedaan moest worden naar de AVG-organisatie, beginselen, privacyrechten en DPIA en datalekken. Er is gekozen in het praktisch onderzoek voor een casestudy. Dit is een vorm van kwalitatief onderzoek waarin verschillende methodieken worden ingezet. In dit geval is gekozen voor een documentenanalyse en een semigestructureerd interview. De documentenanalyse vond plaats om de huidige werkwijze van Lucas Onderwijs in kaart te brengen en dus antwoord te geven op deelvraag 3. Bij de documentenanalyse is er gebruik gemaakt van visueel materiaal, verslagen en flowcharts om een goed beeld te krijgen van de huidige werkwijze van de gegevensverwerking en de implementatie van de AVG. Het semigestructureerd interview vond plaats om te beoordelen of deze huidige werkwijze voldoet aan de AVG-richtlijnen en om gaps op te sporen uit de documentenanalyse. Ter voorbereiding van de interviews zijn interviewvragen en randvoorwaarden opgesteld. Deze zijn meegenomen naar het interview om valide en betrouwbare resultaten te krijgen. De uiteindelijke resultaten van beiden onderzoeken zijn gecombineerd en geven weer in hoeverre de huidige werkwijze van gegevensverwerking voldoen aan de AVG-richtlijnen, en in hoeverre Lucas Onderwijs AVG-Compliant is.

1.8 Leeswijzer

Hoofdstuk 1 begint met de beschrijving van de aanleiding van het onderzoek. In hoofdstuk 2 wordt het literatuuronderzoek behandeld met de Wbp en de AVG, en worden de belangrijke veranderingen uitgelicht. In hoofdstuk 3 wordt de casestudy beschreven welke bestaat uit een documentenanalyse en interview. In dit hoofdstuk komen ook de onderzoeksresultaten aan bod om het proces van gegevensverwerking in kaart te brengen bij Lucas Onderwijs en om te toetsen of deze voldoen aan de AVG. In hoofdstuk 4 worden de conclusies en aanbevelingen naar aanleiding van het onderzoek behandeld, wordt er antwoord gegeven op de centrale onderzoeksvraag en wordt er advies gegeven hoe Lucas onderwijs tot de gewenste situatie kan komen en hoe dit gewaarborgd kan worden.

2. Literatuuronderzoek

Dit hoofdstuk begint met een korte beschrijving van de oude privacywet, de Wet bescherming persoonsgegevens (hierna: Wbp). Daarna zal het huidige juridische kader, de Algemene Verordening Gegevensbescherming (hierna: AVG) in paragraaf 2.2 worden behandeld. Deze paragraaf geeft antwoord op deelvraag 1: “Wat houdt de verordening Algemene Gegevensbescherming in?”. Paragraaf 2.3 tot 2.6 geven antwoord op deelvraag 2: “Waar moet een organisatie aan voldoen om AVG-Compliant te zijn?”.

2.1 Wet Bescherming Persoonsgegevens

In 2018 heeft Lucas Onderwijs zich voorbereid op de AVG-implementatie en in mei 2018 is deze volledig geïmplementeerd. Om de praktische implementatie en veranderingen te volgen in het adviesrapport wordt in deze paragraaf de voorganger, Wet Bescherming Persoonsgegevens (Wbp), besproken.

2.1.1 Organisatie Wet Berscherming Persoonsgegevens

De Wbp gaf regels ter bescherming van de privacy van burgers. De wet was op 1 september 2001 in werking getreden en verving de Wet persoonsregistratie. De Wbp was van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand waren opgenomen of die bestemd waren om daarin te worden opgenomen (art. 2 lid 1 Wbp). De Wbp was van toepassing op de vestigingsplaats van de verantwoordelijke. In welk land de verwerking van gegevens plaats vond was niet relevant. Onder de Wbp was het mogelijk om een Functionaris voor de Gegevensbescherming (hierna: FG) te benoemen, maar dit was niet verplicht. De FG had hierin een adviserende rol en meldde eventuele onregelmatigheden van gegevensverwerking bij de verantwoordelijke of de organisatie waar hij was aangesteld en deed aanbevelingen voor verbeteringen (art. 64 Wbp).

Het toezichthoudend orgaan op de naleving van de Wbp was de Autoriteit Persoonsgegevens (hierna: AP), voorheen het College Bescherming Persoonsgegevens (hierna: Cbp). De AP had de bevoegdheid om bedrijven en overheden te dwingen om zich aan de eisen van de Wbp te houden (art. 52 Wbp). Bij de Wbp werd een verantwoordelijke verplicht om de AP onmiddellijk in kennis te stellen zodra er een ernstige inbreuk op de beveiliging werd geconstateerd. Hierbij kan gedacht worden aan een hackaanval, een technisch falen of verlies van een laptop of andere gegevensdragers waar persoonsgegevens op staan. Voor het niet nakomen van de meldplicht datalekken kon de AP onder de Wbp een bestuurlijke boete op te leggen. Al werd de verantwoordelijke wel eerst in de gelegenheid gesteld om passende beveiligingsmaatregelen te treffen (art. 66 Wbp).

2.1.2 Grondslagen gegevensverzameling

De Wbp bepaalt dat de verwerking van persoonsgegevens in overeenstemming met de wet dient te zijn en dat deze gegevens op behoorlijke en zorgvuldige wijze dienen te zijn verwerkt. Alvorens organisaties overgaan tot gegevensverzameling dient de grondslag te worden bepaald, en kan gerechtvaardigd worden indien deze rust op de zes gronden beschreven in de Wbp (art. 8 Wbp). Volgens de Wbp was de verwerking van persoonsgegevens alleen rechtmatig wanneer er sprake was van tenminste één van de hierna genoemde grondslagen: ondubbelzinnige toestemming, noodzakelijk voor de uitvoering van een overeenkomst, noodzakelijk voor de uitvoering van een wettelijke plicht, noodzakelijk ter vrijwaring van een vitaal belang, noodzakelijk ter vervulling van een publiekrechtelijke taak en noodzakelijk voor het behartigen van een gerechtvaardigd belang.

2.1.3 Het einde van de Wbp

Door de enorme toename van gegevensverwerking en digitalisering door organisaties was er sterke behoefte aan nieuwe privacyrechten en versterking van de bestaande rechten. De Wbp sloot niet meer voldoende aan door deze transitie van digitale gegevensverwerking waarbij de AVG, de nieuwe privacywet, in werking moest treden. De Wbp is per 25 mei 2018 komen te vervallen en hiervoor in de plaats is de AVG-verordening gekomen. Het doel van de AVG komt neer op het versterken van de grondrechten en de fundamentele vrijheden van natuurlijke personen. Dit gaat met name om hun recht op

bescherming van persoonsgegevens en om het vrije verkeer van gegevens binnen de Europese interne markt te beschermen en te waarborgen (art. 1 AVG). Met de invoering van de AVG hebben betrokkenen nieuwe privacyrechten gekregen en werden de bestaande rechten versterkt. Verantwoordelijken die persoonsgegevens verwerken krijgen daarentegen meer verplichtingen. In de volgende paragraaf komen de belangrijke speerpunten van de AVG aan bod.

2.2 Algemene Verordening Gegevensbescherming (AVG)

De AVG, ook wel bekend onder General Data Protection Regulation is een verordening die de regels voor de verwerking van persoonsgegevens regelt. De verordening is van toepassing in de gehele Europese Unie (hierna: EU). De verordening is sinds mei 2016 van toepassing en organisaties hadden tot 25 mei 2018 de tijd om hun bedrijfsvoering in lijn te brengen met deze verordening (Zwenne, & Mommers, 2016). Net zoals de Wbp is de AVG van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen (art. 2 AVG)**.** Met de komst van de AVG zijn de definities van begrippen ten opzichte van de Wbp gewijzigd, en zijn er begrippen gewijzigd waar de definitie ongewijzigd is gebleven om de aanduiding te verscherpen. Daarnaast zijn er nieuwe begrippen geïntroduceerd. In het kader van verduidelijking van deze transitie worden de gewijzigde begrippen behandeld en de nieuwe rol van de FG binnen organisaties.

2.2.1 Begrippen.

Het eerste begrip, persoonsgegevens, is gelijk gebleven, maar de definitie is verscherpt tot alle persoonsgegevens die te herleiden zijn naar een natuurlijk persoon. Artikel 1, lid a geeft de volgende definitie als identificeerbaar:

> Alle informatie over een geïdentificeerde of identificeerbare natuurlijke 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 een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (art. 1, lid a AVG).

Waar de Wbp sprak van een verantwoordelijke, wordt er in de AVG gesproken van een Verwerkingsverantwoordelijke. Artikel 4, lid 7 geeft de definitieert een verwerkingsverantwoordelijke als volgt:

> Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die alleen dan wel samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen (art. 4, lid 7 AVG).

Waar de Wbp sprak van een bewerker, wordt er in de AVG gesproken van een verwerker. De verwerker kan verwerkingsverantwoordelijke zijn in het geval de verwerking van persoonsgegevens binnen dezelfde organisatie plaatsvindt. Aangezien de verwerking van persoonsgegevens uitbesteed kan worden aan een derde partij is het belangrijk om onderscheid te maken binnen deze begrippen. De technische ontwikkelingen op het gebied van gegevensverwerking hebben ervoor gezorgd dat diverse organisaties hebben geïnvesteerd om grote hoeveelheden data te kunnen verwerken. Deze organisaties zijn in de huidige tijd van technische innovaties niet weg te denken en werken samen met verwerkingsverantwoordelijke. Op zowel de verwerkingsverantwoordelijke als de verwerker rust de verantwoordelijkheid tot het nakomen van de plichten die de AVG hen oplegt. Vandaar dat de AVG de

verplichtingen van zowel de verwerkingsverantwoordelijke als de verwerker apart behandelt. Artikel 4 lid 8 AVG definieert de verwerker als: *"*een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt."

2.2.2 Functionaris voor de gegevens bescherming (FG)

In tegenstelling tot de Wbp is het volgens de AVG in een aantal gevallen verplicht om een Functionaris voor de gegevensbescherming (FG) aan te stellen. In onderstaande gevallen is het aanstellen van een FG verplicht, het maakt hierbij niet uit of het om de verantwoordelijke of verwerker gaat.

- indien de verwerker een overheidsinstantie of overheidsorgaan betreft;
- indien de verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen; of
- de verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens (Vermissen, Terstegge & Krijgsman, 2017, p. 40).

Een organisatie met meerdere vestigingen kan één FG benoemen indien de FG vanuit alle vestigingen te benaderen is (art. 37 AVG).

De FG wordt aangewezen op grond van zijn professionele kwaliteiten en deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming. Dat betekent dat de FG goede kennis moet hebben van de privacywetgeving en de processen binnen de organisatie moet kunnen doorgronden (art. 37 lid 5 AVG).

De FG is de centrale contactpersoon binnen de organisatie voor de AVG. De FG helpt structuur aan te brengen door te informeren en adviseren. De organisatie blijft zelf verantwoordelijk voor de naleving van de AVG. De FG dient tijdig te worden betrokken bij aangelegenheden die verband houden met de bescherming van persoonsgegevens. De FG dient derhalve toegang te krijgen tot persoonsgegevens en de verwerkingsactiviteiten en dient de verwerkingsverantwoordelijke en verantwoordelijke de door hem benodigde middelen ter beschikking te stellen om deze taken te kunnen vervullen dan wel zijn kennis tot zijn functie in stand te houden. Om de onafhankelijkheid te waarborgen ontvangt de FG geen instructies tot de uitvoering van zijn taak en geniet hij ontslagbescherming. De FG mag geen andere taken vervullen die tot een belangenconflict kunnen leiden. Artikel 39 van de AVG beschrijft de belangrijkste taken van de FG en is te vinden in bijlage 6. De FG brengt verslag uit aan de hoogste leidinggevende van de verwerkingsverantwoordelijke of de verwerker (art. 38 AVG).

2.3 Beginselen

Hoofdstuk 2 van de AVG onderschrijft 6 beginselen waar organisaties rekening mee dienen te houden bij de verwerking van persoonsgegevens. Dit zijn de beginselen van rechtmatigheid, behoorlijkheid en transparatie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking en integriteit en vertrouwelijkheid. De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van deze beginselen en moet dit kunnen aantonen. In deze paragraaf worden de beginselen nader toegelicht.

2.3.1 Rechtmatigheid, behoorlijkheid en transparantie

Persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant zijn. Dit houdt in dat de persoonsgegevens maatschappelijk verantwoord verwerkt dienen te worden en de verwerkingsverantwoordelijke grondslagen moet kunnen aanwijzen voor het verwerken van persoonsgegevens . Er moet ten minste aan een van de volgene voorwaarden voldaan zijn om de verwerking rechtmatig te achten:

- de betrokkene heeft toestemming gegeven voor een of meer specifieke doeleinden;
- noodzakelijk voor de uitvoering of opstelling van een overeenkomst;
- noodzakelijk om te voldoen aan een wettelijke verplichting;
- noodzakelijk om de vitale belangen van betrokkene of andere natuurlijke personen te beschermen;
- noodzakelijk ter vervulling van een taak van algemeen belang of openbaar gezag;
- noodzakelijk voor de behartiging van de gerechtvaardigde belangen, behalve wanneer de belangen van de betrokkene zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is. Dit geldt niet voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken (art. 6 AVG).

Deze voorwaarden zijn gelijk aan de grondslagen voor gegevensverzameling van de Wbp. Het opmerkelijk verschil hierbij is het feit dat de betrokkene duidelijk toestemming moet geven voor het verwerken van persoonsgegevens. De toestemming moet gegeven worden door een actieve handeling zoals een schriftelijke verklaring of elektronische middelen. Dit betekent niet dat organisaties standaard een beroep kunnen doen op de grondslag toestemming. Toestemming is nodig in het geval dat de wet toestemming eist (marketing) of als de gegevensverwerking indruist tegen de redelijke verwachtingen die en betrokkene mag hebben ten aanzien van privacy. Toestemming vragen betekent dus dat de andere grondslagen niet gebruikt kunnen worden en dus extra goed uitgelegd moet worden waarom verwerking toch nodig is (De IT-jurist, 2017).

Het transparantiebeginsel verplicht de verwerkingsverantwoordelijke om betrokkene te informeren over de eventuele verwerking van zijn persoonsgegevens en met welk doel dit gebeurt, ook wanneer de persoonsgegevens zijn verkregen van derden. Bovendien dient de verwerkingsverantwoordelijke de betrokkene te wijzen op zijn rechten.

2.3.2 Doelbinding
Doelbinding houdt in dat de persoonsgegevens alleen verzameld mogen worden voor een omschreven en gerechtvaardigd doel. Het doel waar de persoonsgegevens voor verzameld zijn is bepalend waar de gegevens voor gebruikt mogen worden. Er mogen niet meer gegevens verwerkt worden dan strikt noodzakelijk is en mogen niet worden gebruikt voor een ander doel (Snijder & de Groot, 2018).

2.3.3 Minimale gegevensverwerking
Volgens het beginsel van minimale gegevensverwerking moeten persoonsgegevens toereikend, terzake dienend en beperkt zijn tot wat noodzakelijk is voor het doeleinde waarvoor de gegevens worden verwerkt. Het is de bedoeling dat de verwerkingsverantwoordelijke alleen die gegevens verwerkt die strikt noodzakelijk zijn voor het vastgestelde doel en kan het doel waarvoor de gegevens worden verwerkt niet op andere wijze worden gerealiseerd (Snijder & de Groot, 2018).

2.3.4 Juistheid
Persoonsgegevens die worden verwerkt dienen juist en actueel te zijn. Indien gegevens niet juist of actueel zijn kan de betrokkene vragen om rectificatie of om de gegevens te wissen. Daarnaast heeft de verwerkingsverantwoordelijke de plicht om te zorgen dat de persoonsgegevens juist zijn en actueel te houden (Snijder & de Groot, 2018).

2.3.5 Opslagbeperking
Het opslagbeginsel moet ervoor zorgen dat persoonsgegevens niet langer bewaard worden dan noodzakelijk is voor de verwerking. Indien er geen wettelijke bewaartermijn van toepassing is dient de verwerkingsverantwoordelijke een passende bewaartermijn vast te stellen voor het doel waar de persoonsgegevens voor verwerkt worden (Snijder & de Groot, 2018).

2.3.6 Integriteit en vertrouwelijkheid

Op het gebied van integriteit en vertrouwelijkheid gelden de uitgangspunten Privacy by design en Privacy by default. Privacy by design houdt in dat organisaties bij het ontwerp van producten en diensten rekening moeten houden met de eisen van de AVG, zoals bescherming en beveiliging van persoonsgegevens en dataminimalisatie. Privacy by default is een uitwerking van het uitgangspunt van de AVG dat de standaardinstellingen van een organisatie altijd zo privacy-vriendelijk mogelijk moeten zijn (Autoriteit Persoonsgegevens, z.j.). Om dit na te leven moeten de verwerkingsverantwoordelijke volgens het integriteit en vertrouwelijkheidsbeginsel technische en organisatorische maatregelen nemen om persoonsgegevens te beveiligen tegen ongeoorloofd toegang of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (Snijder & de Groot, 2018).

2.4 Privacyrechten

In deze paragraaf worden de rechten van betrokkenen beschreven welke in hoofdstuk 3 van de AVG zijn geregeld. Door deze rechten kunnen betrokkenen controle houden over persoonsgegevens. Organisaties dienen gehoor te geven indien betrokkenen beroep doen op hun rechten. De belangrijkste rechten die betrokkenen hebben is het recht op inzage, recht op rectificatie, recht op vergetelheid, recht op beperking van de verwerking en het recht op dataportabiliteit (Zwenne, & Mommers, 2016).

2.4.1 Recht van inzage

De betrokkene heeft het recht om te weten of zijn persoonsgegevens al dan niet worden verwerkt en, indien dit het geval is, heeft betrokkene het recht op inzage van deze persoonsgegevens en het doel waar de gegevens voor worden verwerkt. Bovendien heeft betrokkene het recht om te weten met wie deze persoonsgegevens zijn gedeeld of worden gedeeld en voor welke periode de gegevens zullen worden opgeslagen. Indien de periode niet vooraf kan worden bepaald heeft betrokkene het recht om te weten wat de criteria is om te kunnen bepalen wat de verwachte opslagtermijn zal zijn (Vermissen, Terstegge & Krijgsman, 2017, p. 72).

2.4.2 Recht op rectificatie

De betrokkene heeft het recht om de verwerkingsverantwoordelijke te vragen om onjuistheden in de persoonsgegevens te verbeteren zonder enige onredelijke vertraging. Dit is het geval wanneer de persoonsgegevens niet juist of onvolledig zijn, de persoonsgegevens niet relevant zijn voor het doel waarvoor deze zijn verzameld, of wanneer de wijze van gegevensverwerking in strijd is met een wet (Vermissen, Terstegge & Krijgsman, 2017, p. 73).

2.4.3 Recht op vergetelheid

Een betrokkene heeft in een aantal gevallen het recht op vergetelheid, oftewel het recht om vergeten te worden. Dit houdt in dat betrokkenen de verwerkings-verantwoordelijke kunnen verzoeken om hun persoonsgegevens niet langer te verwerken of op te slaan. De verwerkingsverantwoordelijke dient in onderstaande gevallen hier gehoor aan te geven:

- De opslag van gegevens is niet langer noodzakelijk voor het doel waarvoor deze zijn verzameld.
- De betrokkene trekt een eerder afgegeven toestemming in en er is geen andere wettelijke grondslag voor de verwerking van persoonsgegevens.
- De betrokkene maakt bezwaar tegen het gebruik van zijn persoonsgegevens.
- De verwerking is onrechtmatig. De betrokkene heeft geen toestemming gegeven en er is geen wettelijke grondslag.
- De wettelijk bepaalde bewaartermijn is verlopen.

De verwerkingsverantwoordelijke dient maatregelen te nemen om de gegevens te verwijderen en dient partijen met wie de gegevens zijn gedeeld te informeren dat de gegevens zijn gewist en verzoekt deze partijen dat zij iedere kopie of koppeling naar deze gegevens dienen te verwijderen.

Op het recht op vergetelheid gelden enkele uitzonderingen. Het recht van vergetelheid is niet van toepassing indien de gegevens worden verwerkt:

- voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie;
- om een wettelijke verplichting na te komen, een taak van algemeen belang te vervullen of openbaar gezag uit te oefenen;
- in het belang van de volksgezondheid;
- voor archivering, onderzoek of statistiek;
- In verband met een rechtzaak (Vermissen, Terstegge & Krijgsman, 2017, p. 74).

2.4.4 Recht op beperking

De betrokkene heeft het recht op beperking van de verwerking van persoonsgegevens. Dit is het geval indien betrokkene de juistheid van de persoonsgegevens betwist of wanneer de persoonsgegevens onrechtmatig zijn verkregen. In tegenstelling tot het recht op vergetelheid worden de gegevens niet verwijderd. De betrokkene kan zich beroepen op het beperken van gegevensverwerking indien betrokkene de gegevens later kan opvragen, bijvoorbeeld wanneer de gegevens nodig zijn voor een rechtsvordering. De betrokkene kan bovendien bezwaar indienen tegen de verwerking van zijn persoonsgegevens. De verwerkingsverantwoordelijke mag de persoonsgegevens niet verwerken tenzij er dwingende gerechtvaardigde gronden voor de verwerking zijn die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene (Vermissen, Terstegge & Krijgsman, 2017, p. 75).

2.4.5 Recht op dataportabiliteit

De betrokkene heeft het recht op dataportabiliteit. Dit houdt in dat de verwerkingsverantwoordelijke de plicht heeft om gegevens over te dragen indien de betrokkene hierom vraagt. Het gaat hierbij om gedigitaliseerde gegevens die met toestemming van betrokkene of krachtens een overeenkomst met betrokkene worden verwerkt. De gegevens dienen in een gestructureerde, gangbare en machineleesbare vorm te worden verstrekt. De betrokkene heeft hierbij de keuze om deze gegevens zelf te ontvangen dan wel de verwerkingsverantwoordelijke te verzoeken de gegevens over te dragen aan een andere verwerkingsverantwoordelijke (Vermissen, Terstegge & Krijgsman, 2017, p. 74).

2.5 DPIA en datalekken

De AVG verplicht om een Data Protection Impact Assesment (DPIA), ook wel Privacy Impact Assesment (PIA) uit te voeren bij een nieuwe vorm van gegevensverwerking en wanneer dit waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen oplevert. De verwerkingsverantwoordelijke dient een DPIA uit te voeren voordat de nieuwe vorm van gegevensverwerking plaats vindt. Pas als de risico's zijn weggenomen mag de verwerking plaatsvinden. Een DPIA dient de volgende informatie te bevatten (art. 27 AVG).

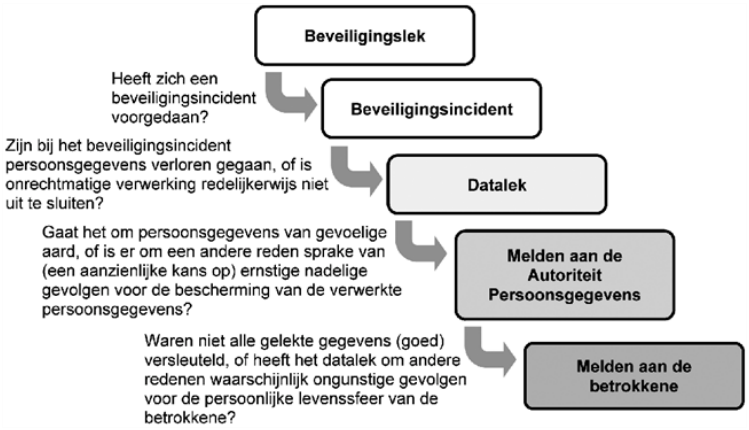
- Een algemene beschrijving van de beoogde verwerkingen en het doel daarvan.
- Een beoordeling van de grondslag en de noodzaak van de gegevensverwerking.
- De risico's van de verwerkingen voor de rechten en vrijheden van de betrokkenen.
- De voorgenomen maatregelen om de persoonsgegevens te beschermen tegen de risico's

Datalekken

De meldplicht datalekken is op 1 januari 2016 onder de Wbp ingegaan. De meldplicht houdt in dat de verwerkingsverantwoordelijke verplicht is om melding te doen van een datalek bij de AP. De meldplicht is onder de AVG aangescherpt. De melding moet zonder enige vertraging en uiterlijk binnen 72 uur gebeuren (Autoriteit Persoonsgegevens, 2018). Er hoeft geen melding te worden gedaan indien er geen risico op de inbreuk voor de rechten en vrijheden van personen aanwezig is. Het datalek moet daarnaast ook worden gemeld aan de betrokkene indien het waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. De verwerkinmgsverantwoordelijke is verplicht om een incidentenregister bij te houden waarin tevens de genomen maatregelen in zijn opgenomen. De AP kan om inzage vragen van het

incidentenregister om de naleving op de meldingsplicht datalekken te controleren (Vermissen, Terstegge & Krijgsman, 2017, p. 49).

Er is sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan waarbij persoonsgegevens verloren zijn gegaan, of als onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs uitgesloten kunnen worden.
Met behulp van schema 2.1 kan bepaald worden of er sprake is van een datalek en wie hierover geinformeerd moeten worden.



Schema 2.1: Datalek

2.6 Implementatie van de AVG

De autoriteit persoonsgegevens heeft richtlijnen en hulpmiddelen gepubliceerd om organisaties te helpen aan de AVG te voldoen. De AP-checklist is een 10-stappenplan om een organisatie te helpen voorbereid te zijn op de AVG (Autoriteit Persoonsgegevens, z.j.). Het stappenplan is aanvankelijk bedoeld om organisaties te helpen met de toetsing aan de AVG, maar is een geschikte leidraad om te bepalen of de huidige organisaties de AVG-regels omarmen. Deze is te vinden in bijlage 10. Om er zeker van te zijn dat het empirisch model volstaat, worden de stappen hieronder behandeld en als leidraad genomen als de AVG-topics.

Stap 1: Bewustwording: Alle relevante personen moeten op de hoogte zijn van de nieuwe privacywetten en de impact op alle processen, diensten en goederen. De Autoriteit Persoonsgegevens (AP) biedt instrumenten die kunnen helpen om de AVG na te leven zoals guidelines en men moet bewust zijn van de sancties.

Stap 2: Rechten van betrokkenen: Betrokkenen hebben met de AVG meer rechten gekregen ten aanzien van de Wbp. De organisatie moet ervoor zorgen dat zij op de hoogte zijn van al deze rechten en of men zich hieraan houdt. Bovendien is het belangrijk om te te kijken hoe de organisatie met de gegevens omgaat.

Stap 3: Overzicht verwerkingen: Met de rechten van de betrokkenen, en de verantwoordingsplicht moeten de gegevensverwerkingen in kaart gebracht worden met de categorie van gegevens op basis van wettelijke grondslag waar deze op zijn verwerkt. Grondslagen zijn grotendeels hetzelfde met de Wbp.

Stap 4: Data Protection Impact Assessment. Onder de AVG kan het verplicht zijn een Data Protection Impact Assessment (DPIA) uit te voeren. Dit instrument is behandeld in 3.4. Organisaties moeten nagaan of dit verplicht is voor hen.

Stap 5: Privacy by design & privacy by default. De organisatie moet vertrouwd worden met de onder de AVG verplichte uitgangspunten van *privacy by design* en *privacy by default* en nagegaan moet worden hoe deze beginselen ingevoerd worden.

Stap 6: Functionaris voor de gegevensbescherming. Onder de AVG kunnen organisaties verplicht zijn om een functionaris voor de gegevensverwerking (FG) aan te stellen. Bepaald moet worden of dit voor de organisatie geldt.

Stap 7: Meldplicht datalekken. De meldplicht datalekkenblijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan de eigen registratie van de datalekken die zich in de organisatie hebben voorgedaan. Alle datalekken moeten gedocumenteerd worden. Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan. Dit gaat verder dan de huidige protocolplicht uit de Wbp, die alleen betrekking heeft op de gemelde datalekken.

Stap 8: Bewerkersovereenkomsten. Als de gegevensverwerking uitbesteed is aan een Bewerker (in de AVG 'verwerker' genoemd) dan moet beoordeeld worden of de overeengekomen maatregelen in bestaande contracten met uw bewerkers nog steeds toereikend zijn en voldoen aan de vereisten in de AVG.

Stap 9: Leidende toezichthouder: Als een organisatie vestigingen (of andere impact) heeft in meerdere EU-lidstaten dan hoeft er met nog maar één privacytoezichthouder zaken gedaan te worden, de leidende toeichthouder. De organisatie moet nagaan of dit geldt en zo ja onder welke privacytoezichthouder het dan valt.

Stap 10: Toestemming. Voor sommige gegevensverwerkingen is toestemming nodig van de betrokkenen. De AVG stelt strengere eisen aan toestemming. De manier waarop toestemming gevraagd wordt moet geevalueerd worden. Er moet met de AVG aangetoond kunnen worden dat er geldige toestemming verkregen is om persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven.

2.7 Conclusie

In dit hoofdstuk is antwoord gegeven op deelvragen 1 en 2. Het uitgevoerde literatuuronderzoek is beschreven waarbij de belangrijkste veranderingen die de AVG met zich meebrengt zijn uitgelicht. Het belangrijke verschil van de AVG-verordening met de Wbp is dat de Wbp een uitwerking was van de europese richtlijn. De AVG-verordening heeft direct werking op alle EU landen. De AVG-verordening laat ook minder ruimte voor eigen invulling van nationale wetgeving. Met de komst van de AVG zijn de definities van begrippen ten opzichte van de Wbp gewijzigd, zijn er begrippen gewijzigd en zijn er nieuwe begrippen geintroduceerd. Dit was noodzakelijk om aan te sluiten bij de huidige tijd van technologische informatievoorziening. Bovendien is het aanstellen van een Functionaris voor de Gegevensbescherming (FG) in een aantal gevallen verplicht.

Onder de AVG hebben organisaties meer verantwoordelijkheden gekregen waar zij zich aan dienen te houden om AVG-compliant te zijn. Voor elke verwerking dient de verwerkingsverantwoordelijke toestemming te vragen en moet in duidelijke taal worden gecommuniceerd. De organisatie dient rekening te houden met de beginselen bij het verwerken van de persoonsgegevens. Dit zijn de beginselen van rechtmatigheid, behoorlijkheid en transparatie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking en integriteit en vertrouwelijkheid. De betrokkene dient bovendien op zijn rechten te worden gewezen. Onder de AVG zijn de rechten van betrokkenen versterkt en zijn er rechten bijgekomen. De vijf belangrijke rechten die betrokkenen hebben is het recht op inzage, rectificatie, vergetelheid, dataportabiliteit en de beperking van gegevensverwerking. Deze rechten maakt het voor betrokkenen mogelijk om invloed uit te oefenen op wat er met hun gegevens gebeurt. Organisaties moeten tevens aan kunnen tonen dat zij technische en organisatorische maatregelen hebben genomen om persoonsgegevens te beveiligen tegen ongeoorloofd toegang of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. In het geval van een datalek is het verplicht dit te melden bij de AP en moet dit gedocumenteerd worden. Ten slotte dienen organisaties bij een nieuwe vorm van gegevensverwerking een Data Protection Impact Assesment (DPIA) uit te voeren. Pas als alle onaanvaardbare risico's zijn weggenomen kan een nieuwe gegevensverwerking plaatsvinden.

3. Onderzoeksmethoden en huidige situatie

In dit hoofdstuk wordt een kwalitatief onderzoek uitgevoerd en wordt de huidige situatie van Lucas Onderwijs geanalyseerd met betrekking tot de AVG. Het onderzoeksplan is ontworpen om binnen Lucas Onderwijs de geformuleerde onderzoeksvraag te beantwoorden. De onderzoeksmethoden, dataverzameling, validiteit, betrouwbaarheid en onderzoekspopulatie en steekproef worden in paragraaf 3.1 behandeld. Vervolgens worden de onderzoeksresultaten behandeld in paragraaf 3.2.

3.1 Onderzoeksmethoden

Centraal in het onderzoek staat het in kaart brengen van de huidige werkwijze ten aanzien van de verwerking van persoonsgegevens en de beoordeling of deze werkwijze voldoet aan de AVG-richtlijn. De punten waar onderzoek naar gedaan is moeten dus beoordelen of deze voldoen aan de AVG-richtlijn. In het theoretisch kader zijn de elementen Organisatie, Beginselen, Privacyrechten en DPIA en Datalekken aan bod gekomen die de AVG-compliance behandelen. In deze volgorde is er een model ontwikkeld dat moet oordelen of Lucas Onderwijs AVG-Compliant is. Er is gebruik gemaakt van het 10-stappenplan van de AP uit hoofdstuk 2.6 om hetgeen te operationaliseren. De stappen zijn onder de elementen gegroepeerd, en vormen de topics voor het onderzoek. De ontwikkelde vragenlijsten zijn gebaseerd op deze elementen en topics.

Organisatie van de AVG
•Stap 1: Bewustwording •Stap 6: FG •Stap 8: Bewustwording overeenkomst •Stap 9: Leidende toezichthouders (Niet van toepassing voor Lucas Onderwijs)
Beginselen
•Stap 5: Privacy by design & Privacy by default
Privacyrechten
•Stap 2: Rechten van betrokkenen •Stap 3: Overzicht verwerkingen •Stap 10: Toestemming
DPIA en datalekken
•Stap 4: Data protection impact assessment •Stap 7: Datalek

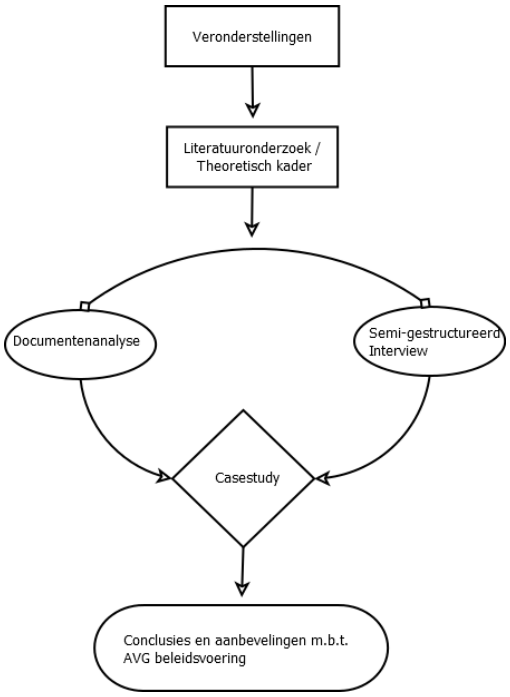
Tabel 3.1: AVG-elementen met het stappenplan

In 3.1.1 is de keus voor een casestudy uitgewerkt als dataverzamelingsmethode, 3.1.2 behandelt de onderzoekspopulatie en steekproefverantwoording van de interviews, en 3.1.3 behandeld validiteit en betrouwbaarheid van de interviews met de genomen maatregelen voor stabiele onderzoeksresultaten.

3.1.1 Casestudy

Een casestudy is een kwalitatieve dataverzamelingsmethode waarmee één onderzoekseenheid, één case, onderzocht wordt in zijn omgeving. De onderzoekseenheid kan een persoon, organisatie of systeem zijn. Een casestudy is breed toepasbaar en hierbij worden meerdere dataverzamelingsmethoden gecombineerd (triangulatie). Een casestudy is goed inzetbaar voor beschrijvend- en verklarend onderzoek (Saunders, Lewis, & Thornhill, 2009, p. 146).

Het doel van dit onderzoek is eveneens om gedetailleerde beschrijvingen en verklaringen te verkrijgen op het gebied van AVG en gegevensverwerking. In dit onderzoek is er gekozen voor de casestudy aangezien er wordt gericht op een probleemstelling waar behoefte is aan verschillende inzichten, en triangulatie dus gewenst is. De casestudy richt zich in dit onderzoek tot enerzijds een documentenanalyse waarin de verwerking van persoonsgegevens in kaart wordt gebracht bij Lucas Onderwijs. Anderzijds richt de casestudy zich tot een interview waarin respondenten geïnterviewd worden die betrokken zijn bij de AVG met als doel om te beoordelen of de verwerking van persoonsgegevens voldoet aan de AVG-richtlijn. De onderzoeksopzet is visueel afgebeeld in figuur 3.1. De dataverzamelingsmethoden worden in deze sub-paragraaf verder uitgelicht.



Figuur 3.1 Onderzoeksopzet

Dataverzameling: Documentenanalyse.
Met een documentenanalyse wordt de inhoud van bestaande informatie geanalyseerd. Het doel van de documentenanalyse is om een verschijnsel te beschrijven of te verklaren door op systematische en effectieve manier gegevens te verzamelen over het onderwerp. Om zo efficiënt mogelijk te analyseren worden vooraf de variabelen bepaald van de documenten die worden onderzocht. De documentenanalyse is een verkennende kwalitatieve dataverzamelingsmethode, en is te gebruiken voor tekstmateriaal en visueel materiaal (Saunders, Lewis, & Thornhill, 2009, p. 147).
Er is gekozen voor een documentenanalyse omdat er voldoende informatie beschikbaar is om de implementatie en de organisatie van de AVG in kaart te brengen van Lucas Onderwijs. De documentenanalyse moet antwoord geven op deelvraag 3: “Wat is de huidige werkwijze van Lucas onderwijs ten aanzien van de verwerking van persoonsgegevens?”. Met de documentenanalyse is de inhoud van bestaande beschikbare documenten op het gebied van AVG geanalyseerd. Om betrouwbaarheid van de documenten te waarborgen zijn informatiedocumenten geraadpleegd die geschreven zijn door Lucas Onderwijs en afkomstig zijn van de HRM adviseur, salarisadministrateur, unitleider personeel en salarisadministratie en de Security Officer. De geraadpleegde bronnen zijn onder meer gepubliceerde verslagen bij de implementatie van de AVG, communicatiemateriaal naar medewerkers, en flow-charts. Om efficiënt te analyseren wordt er in het onderzoek gericht op documenten met betrekking tot de implementatie en organisatie van de AVG en de processen bij het verwerken van personeelsgegevens.

Dataverzameling: Semigestructureerd interview.
Informatie uit de documentenanalyse is positief gepresenteerd en situaties waarin AVG-regels worden overtreden worden hier niet in vastgelegd. Met behulp van het interview zijn de gaps opgespoord van de documentenanalyse. De interviews hebben plaatsgevonden na de documentenanalyse en hebben als doel om antwoord te geven op deelvraag 4: “Voldoet de huidige werkwijze aan de AVG-richtlijn?”

Met behulp van interviews is het mogelijk om de diepte in te gaan en nieuwe inzichten te verzamelen over bepaalde topics. Interviewsoorten voor een kwalitatief onderzoek zijn een ongestructureerd interview, een semigestructureerd interview en een focusgroep. Bij een semigestructureerd onderzoek wordt een interviewschema opgesteld met algemeen geformuleerde vragen, maar hier mag wel van afgeweken worden om door te kunnen vragen bij interessante uitspraken van de respondent of wanneer antwoorden niet duidelijk zijn (Saunders, Lewis, & Thornhill,2009, p. 320). Hiermee wordt meer gedetailleerde informatie verkregen wat in dit onderzoek het doel is. In het interview moest het thema vast staan, namelijk AVG en personeelsgegevensverwerking. Het is in het interview wenselijk om van de vragenlijst af te kunnen wijken om door te vragen bij interessante antwoorden of opmerkingen die van belang kunnen zijn bij het beoordelen of er overtredingen plaats hebben gevonden in het afgelopen jaar. In het onderzoek is er daarom gekozen voor semigestructureerde interviews.

Er heeft een interview plaatsgevonden met mevr. D. Rogier (HRM Adviseur) en dhr. F. Bos (Security Officer). Voor het interview is gebruik gemaakt van de topiclijst uit tabel 3.1. Er is gesproken over de organisatie en de implementatie van de AVG, de beginselen, de privacyrechten van de werknemers en de DPIA en datalekken. In het interview is gebruik gemaakt van de interviewvragenlijsten en randvoorwaarden welke te vinden zijn in bijlage 3. Aangezien de HRM adviseur en Security Officer expert zijn op eigen vakgebied, is de vragenlijst toegespitst op 2 verschillende interviewvragenlijsten. Er is voor beide interviewvragenlijsten gezorgd dat de vragen opbouwend zijn van makkelijk naar moeilijkere vragen zodat de respondent zich meer in zal leven in het onderwerp. De belangrijkste antwoorden zijn vervolgens getranscribeerd en zijn te vinden in bijlage 4 en 5. Hierna heeft een analyse plaatsgevonden (hoofdstuk 3.2) en zijn de relevante uitspraken geparafraseerd.

3.1.2 Onderzoekspopulatie en steekproef

Om het aantal respondenten voor het interview te bepalen is het van belang vast te stellen of de resultaten gegeneraliseerd moeten worden. In het geval van een casestudy is het niet zo dat meer interviews altijd beter is. Dit is alleen van belang zolang er nieuwe informatie wordt verzameld (Vleeshouwer, 2017). Het is wel belangrijk dat de relevante mensen geïnterviewd worden. De interviews zijn onderdeel van een casestudie, en het onderzoek richt zich op deze specifieke AVG-case. Dit betekent dat de uiteindelijke resultaten niet gegeneraliseerd hoeven te worden. Op het moment dat er geen nieuwe informatie ingewonnen kan worden door de theoretische saturatie zijn er genoeg mensen geïnterviewd. Van belang hierbij is dus wel dat de relevante mensen geïnterviewd worden. Op basis van de topics en vragenlijsten is bewust gekozen voor interviews met de HRM adviseur en Security Officer. Alleen zij beschikken over de kennis om antwoord te kunnen geven op de vragen die leidend zijn voor het beantwoorden van de centrale onderzoeksvraag.

3.1.3 Validiteit en betrouwbaarheid

Dataverzameling dient op een betrouwbare en valide manier te worden uitgevoerd. De betrouwbaarheid van een onderzoek draait om het tot een minimum beperken van toevallige fouten. De validiteit van een onderzoek gaat in op het voorkomen van systematische fouten (Swaen, 2014).

Interne validiteit
De interne validiteit is de mate waarin het onderzoek goed is opgezet en uitgevoerd zodat conclusies voor waar aangenomen kunnen worden (Swaen, 2014). Het gaat er hier om dat de juiste vragen gesteld worden die het onderwerp omvatten. Om de interne validiteit te borgen in de interviews zijn de volgende maatregelen genomen:

- De interviewvragen en randvoorwaarden zijn opgesteld en worden meegenomen naar het interview (bijlage 4).
- De interviewvragen zijn gecontroleerd door een tweede lezer.
- De interviewvragen zijn gebaseerd op het onderzoeksmodel.
- De geïnterviewden mogen zelf beslissen of de vragen anoniem beantwoord worden zodat de kans op wenselijke antwoorden wordt verlaagd.
- De interviews worden opgenomen en volledig uitgeschreven voordat er verbanden en conclusies worden getrokken.
- De getranscribeerde interviews worden na afloop nog aan de geïnterviewden voorgelegd om na te gaan of hetgeen erin staat klopt met wat de geïnterviewden wilden zeggen.

Externe validiteit

De externe validiteit is de mate waarin de onderzoeksresultaten te generaliseren zijn naar andere situaties of cases dan die van het onderzoek, ofwel de mate waarin ze te generaliseren zijn over de gehele populatie. De externe validiteit van het interview is positief te beïnvloeden door voldoende respondenten te gebruiken en deze willekeurig te selecteren zodat de resultaten te generaliseren zijn naar een grotere populatie. Zoals beschreven staat in de verantwoording van de onderzoekspopulatie en steekproef vinden de interviews plaats om onderzoek te doen naar een specifieke case, namelijk AVG binnen Lucas Onderwijs. Het generaliseren van de bevindingen is hierbij geen doel. Externe validiteit is in dit geval dus minder belangrijk (Swaen, 2014).

Betrouwbaarheid

Het onderzoek is vatbaar voor fouten die de betrouwbaarheid van de resultaten verlagen. In dit kwalitatief onderzoek zijn betrouwbaarheidseisen van toepassing. Indien aan deze eisen wordt voldaan, wordt het onderzoek betrouwbaarder ondervonden (Swaen, 2014). Om de betrouwbaarheid te vergroten zijn de volgende maatregelen genomen:

- Voor de documentenanalyse is er uitsluitend gebruik gemaakt van documenten die geschreven zijn door Lucas Onderwijs en afkomstig zijn van de HRM adviseur, salarisadministrateur, unitleider personeel en salarisadministratie en de Security Officer.
- De achtergrond van het onderzoek en de toegevoegde waarde werden toegelicht tijdens het interview.
- Er werden verschillende onderzoeksmethoden gebruikt ter beantwoording van de onderzoeksvraag (triangulatie), namelijk documentenanalyse en een interview.
- Er werd gebruikgemaakt van semigestructureerde interviews, met een vragenlijst.
- De interviews hebben plaatsgevonden bij Lucas Onderwijs in een gesloten ruimte waar niet gestoord kan worden.
- De respondenten zijn geïnformeerd dat het interview 1 uur zal duren.
- De respondent werd verteld dat hij/zij mag onderbreken voor vragen of verduidelijking.
- De te stellen vragen zijn duidelijk en vriendelijk geformuleerd zodat zij vrij uit konden vertellen over de processen en zij zich niet hoefden te verdedigen.
- Tijdens het interview werd geanticipeerd op non-verbale signalen zoals afwezigheid of nerveusiteit en indien nodig werd de respondent met zijn volledige aandacht terug bij het interview gehaald.
- Er wordt doorgevraagd bij de respondent bij omslachtige of onduidelijk antwoorden door voorbeelden aan te halen, samen te vatten of om een bevestiging te vragen.
- Tussendoor werd er gecontroleerd of de opname nog lien en was er een koffiemoment.
- Nadat een topic werd behandeld werd deze samenvattend geconcludeerd.

3.2 Onderzoeksresultaten

In deze paragraaf worden de onderzoeksresultaten gepresenteerd en geanalyseerd welke zijn verzameld met de documentenanalyse en interviews. In de volgorde van AVG-organisatie, Beginselen, Privacyregels en DPIA en Datalekken worden deze behandeld.

3.2.1 AVG-organisatie

Voorbereidingen AVG.

Lucas Onderwijs is halverwege 2017 met de voorbereidingen gestart voor het AVG-proof maken van de organisatie. Met ingang van januari 2018 is een projectgroep opgezet onder leiding van de directeur van het stichtingsbureau. Vanwege de omvang en structuur van de organisatie is gekozen om een Security Officer te benoemen. Hierdoor hoeven de scholen geen AVG-specialist in dienst te nemen. De security officer bij Lucas Onderwijs heeft voldoende kennis van de AVG en de organisatie kan terecht bij de Security Officer met vragen. Meer hierover bij “Aanstelling Functionaris Gegevensbescherming en Security Officer”.

Bij de implementatie van de AVG is een onderscheid gemaakt in een drietal gebieden:

1. De bewustwording bij medewerkers.
2. De formele zaken (dataregisters, verwerkingsovereenkomsten, protocollen etc.).
3. De technische zaken (bescherming tegen aanvallen, instellingen van wachtwoorden, beveiliging van applicaties, etc.).

Ad 1 Bewustwording

Lucas onderwijs is zich privacy bewust omdat Lucas onderwijs zich aan de wet moet houden en moet kunnen aantonen dat zij aan de AVG voldoet. Om de bewustwording onder de medewerkers onder de aandacht te brengen is vanuit het bestuur regelmatig gecommuniceerd d.m.v. presentaties en nieuwsbrieven. Om dit proces te ondersteunen is een flyer gemaakt waarin medewerkers handvatten wordt geboden hoe zij moeten omgaan met persoonsgegevens**.** De flyer is te vinden in bijlage 2. Aan de medewerkers werd tevens trainingen aangeboden om de bewustwording te vergroten. In deze cursussen wordt medewerkers uitgelegd wat je als medewerker moet weten over de AVG en hoe je de privacy van leerlingen en collega’s kunt beschermen. Na de cursus zijn medewerkers in staat om onder andere persoonsgegevens te kwalificeren en wanneer persoonsgegevens mogen worden uitgewisseld.

Ad 2 Formele zaken

Met de introductie van de AVG is er een Privacyreglement Stichting Lucas Onderwijs opgesteld, deze is te vinden in bijlage 7. In dit reglement zijn alle richtlijnen voor het verwerken van gegevens opgenomen, en geldt voor de gehele organisatie. Bij de invoering van de AVG zijn de reeds bestaande protocollen met betrekking tot het verwerken van persoonsgegevens in overeenstemming met de AVG gebracht, en zijn er nieuwe protocollen en handreikingen gepubliceerd. De volgende relevante protocollen met betrekking tot AVG zijn gepubliceer door LucasOnderwijs:

- Privacyreglement Stichting Lucas Onderwijs
- Protocol Datalekken Stichting Lucas Onderwijs
- Handreiking AVG en Verzuim
- Responsible Disclosure
- Gedragscode verantwoord gebruik ICT en internet

Lucas onderwijs is verantwoordelijk voor de zorgvuldige omgang van persoonsgegevens. Om dit te kunnen garanderen zijn afspraken gemaakt met de verwerkers. Deze afspraken worden in een verwerkingsovereenkomst vastgelegd. De verwerkingsovereenkomsten worden afgesloten op bestuurlijk niveau. Alleen overeenkomsten ondertekend door het College van Bestuur (hierna: CvB) en de verwerker zijn rechtsgeldig. Lucas Onderwijs is begin 2018 begonnen met 20 verwerkersovereenkomsten en dat zijn er in juli 2019 170 geworden. Er zijn ook organisaties die persoonsgegevens van Lucas Onderwijs verwerken en die zelf verwerkingsverantwoordelijke zijn. Deze organisaties hebben hiervoor een eigen doelbinding en een wettelijke grondslag om deze gegevens te mogen ontvangen en te verwerken. Voorbeelden hiervan zijn Dienst Uitvoering Onderwijs (DUO) en de belastingdienst.

Ad 3 Technische zaken
Als onderdeel van de invoering van de AVG is een nieuw wachtwoordbeleid opgesteld voor alle medewerkers van Lucas Onderwijs. In sommige situaties wordt dit afgedwongen door de applicaties. Binnen de organisatie worden systemen gebruikt die zodanig zijn ontworpen dat de rechten door de organisatie worden bepaald. (Privacy bij default). In de rapportagetool Capisci zijn de rollen vooraf door de leverancier bepaald (privacy by design).

Medewerkers wordt geacht dat zij zich aan het wachtwoordbeleid houden. Voor zover mogelijk wordt met een dubbele authenticatie ingelogd waarbij naast een gebruikersnaam en wachtwoord er nog een extra code nodig is om toegang te krijgen. Deze functionaliteit is tot op heden alleen toegepast op het Identity en Acces Managementsysteem. Om wachtwoorden te onthouden adviseert Lucas Onderwijs medewerkers gebruik te maken van passwordmanagers die tevens veilige wachtwoorden kunnen genereren. Persoonsgegevens worden alleen uitgewisseld indien er een beveiligde verbinding is. Dat garandeert dat de gegevens tussen de verzender en ontvanger versleuteld zijn. Lucas Onderwijs ziet ook toe op het regelmatig installeren van updates om de beveiliging van systemen te waarborgen.

Aanstelling Functionaris Gegevensbescherming en Security Officer. Lucas onderwijs is volgens de AVG verplicht om een functionaris voor gegevensbescherming aan te stellen. Lucas onderwijs voldoet aan twee van de drie criteria die het aanstellen van een FG verplichten. Lucas Onderwijs kan namelijk worden aangemerkt als een publieke organisatie en Lucas Onderwijs verwerkt op grote schaal bijzondere persoonsgegevens. Lucas Onderwijs heeft de heer Y. Bleeker met ingang van 25 mei 2018 aangesteld als FG. De heer Y. Bleeker is gepensioneerd en heeft geen andere functie binnen Lucas Onderwijs. Lucas onderwijs heeft bewust gekozen voor een interne FG. Een interne FG is goed bekend met de eigen organisatie, waardoor er snel geschakeld kan worden. De FG heeft een adviserende en controlerende taak, heeft een ontslagbescherming en heeft verregaande bevoegdheden. Bij ernstig falen mag de FG buiten het CvB handelen. Naast de FG heeft de organisatie de heer F. Bos benoemd als Security Officer. De heer F. Bos is werkzaam als IT-specialist en beheert de netwerken en ICT van een aantal scholen van Lucas Onderwijs. De keuze voor een Security Officer is omdat de AVG veel uitvoering met zich meebrengt. In tegenstelling tot de FG heeft een Security Officer geen ontslagbescherming. De Security Officer heeft een uitvoerende taak en rapporteert aan de FG. De Security Officer is verantwoordelijk voor de verwerkersovereenkomsten en is het aanspreekpunt binnen de organisatie voor alle vragen met betrekking tot de AVG. De Security Officer heeft tevens de taak om een DPIA uit te voeren. De Security Officer houdt een dataregister bij van verwerkersovereenkomsten, incidentenregister en de verwerkingen die binnen de organisatie plaatsvinden.

3.2.2 Beginselen

Rechtmatigheid, behoorlijkheid en transparantie
Er zijn voldoende grondslagen die bepalen dat de persoonsgegevens verwerkt mogen worden. De verwerking is noodzakelijk voor de uitvoering van een arbeidsovereenkomst om betrokkene te kunnen verlonen. De verwerking van persoonsgegevens is tevens noodzakelijk voor het nakomen van een wettelijke verplichting. De verwerking van persoonsgegevens van personeelsleden is noodzakelijk voor de berekening van de te betalen loonbelasting, de af te dragen pensioenpremies en voor de afdracht van werknemersverzekeringen. Bovendien worden alleen die gegevens verwerkt die werknemers zelf aanleveren. De persoonsgegevens worden niet verwerkt voor andere doeleinden. Met instemming van de Medenzeggenschapsraad heeft Lucas Onderwijs de personeelsdossiers gedigitaliseerd en zijn alle medewerkers op de hoogte gebracht. Alle medewerkers hebben hier een e-mail bericht over ontvangen. Medewerkers is gevraagd om de inhoud van hun personeelsdossier te controleren en kunnen zij bezwaar maken indien hierin documenten zijn opgenomen waar zij het niet mee eens zijn. Het is leidinggevenden niet toegestaan om gegevens van medewerkers omtrent hun gezondheid vast te leggen. Medewerkers mogen dit wel met hun leidinggevende delen, maar zij mogen hier niet naar vragen. Ook het informeren van collega's of zakelijke relaties over de afwezigheid en de ziekte van een medewerker door de

leidinggevende is niet toegestaan. Indien de medewerker informatie wil geven, dan moet de medewerker dit op persoonlijke titel via persoonlijke communicatiemiddelen doen, door bijvoorbeeld collega's zelf te e-mailen.

Doelbinding
Lucas onderwijs verwerkt persoonsgegevens uitsluitend voor zover de verwerking verenigbaar is met de omschreven doelen en verwerkt niet meer gegevens dan noodzakelijk is om de betreffende doelen te bereiken. De grondslag voor Lucas Onderwijs om persoonsgegevens te verwerken ten aanzien van haar medewerkers is de uitvoering van een overeenkomst. De verwerking van persoonsgegevens uit de arbeidsovereenkomst is noodzakelijk voor de verloning van medewerkers. Aan de verwerking van persoonsgegevens van medewerkers ligt tevens een wettelijke grondslag. Om belastingen en premies te berekenen en af te dragen is de verwerking noodzakelijk. Lucas Onderwijs verzamelt en verwerkt geen persoonsgegevens zonder dat medewerkers daar specifiek toestemming voor gegeven hebben. Bij het actualiseren van het smoelenboek is alle medewerkers uitdrukkelijk om toestemming gevraagd om hun gegevens te mogen opnemen in het smoelenboek. Medewerkers hebben toestemming gegeven door middel van een brief met handtekening.

Minimale gegevensverwerking
Volgens het beginsel van minimale gegevensverwerking moeten de persoonsgegevens toereikend, terzake dienend en beperkt zijn tot wat noodzakelijk is voor het doeleinde waarvoor de gegevens worden verwerkt. Bij dataminimalisatie wordt kritisch gekeken naar de data en wordt bepaald wat noodzakelijk is voor de verwerking en of de gegevens niet langer bewaard worden dan nodig is. Bij de gegevensverzameling van nieuwe medewerkers is onduidelijk welke gegevens nodig zijn. Het is niet duidelijk waarom de gegevens van een partner of het geslacht worden gevraagd. Volgens Desiree Rogier, HRM adviseur bij Lucas Onderwijs is het voldoende voor het pensioenfonds om te weten of een medewerker een partner heeft en is de leeftijd van de partner niet relevant.

Juistheid
Lucas onderwijs heeft de personeelsdossiers per oktober 2018 gedigitaliseerde en is er geen papieren personeelsdossier meer aanwezig. In dit personeelsdossier worden alle gegevens van een personeelslid opgeslagen met betrekking tot zijn dienstbetrekking. Op grond van de juistheidsbeginsel rust de plicht op Lucas onderwijs om te zorgen dat de gegevens juist en actueel zijn. Een personeelslid kan om rectificatie vragen indien de gegevens onjuist zijn of vragen om de gegevens te wissen wanneer het personeelslid uit dienst treedt. Veelal is het mogelijk voor een personeelslid zelf direct wijzigingen aan te brengen. Meer hierover in "recht op rectificatie" op de volgende pagina.

Opslagbeperking
Lucas Onderwijs hanteert de wettelijke bewaartermijn voor zover dat van toepassing is. Er zijn een aantal wettelijke bewaartermijnen die een eigen wettelijke grondslag kennen. De Security Officer heeft deze in kaart gebracht en de wettelijke grondslag met wetsartikelen erbij gezet.

Uit het interview met de Security Officer Fons Bos blijkt dat de systemen die Lucas Onderwijs gebruikt niet mogelijk is om een classificatie te maken van de bewaartermijn. Dit geld voor het Document Management Systeem (hierna: DMS) en het Identity Acces managementsysteem (hierna: IAS) waarin de toegang geregeld wordt tot systemen en waar tevens e-mails worden aangemaakt.
Naast deze systemen worden personeelsgegevens per e-mail uitgewisseld binnen de organisatie. De Security Officer zegt dat er geen regels zijn met betrekking tot de houdbaarheid van emailberichten die persoonsgegevens bevatten. Daarnaast komt het voor dat bestanden met personeelsgegevens op een lokale schijf worden opgeslagen waardoor niet toegezien kan worden op de bewaartermijn.
RAET is momenteel bezig om de digitale personeelsomgeving Youforce te voorzien van een bewaartermijn classificatie. Documenten kunnen dan worden opgeslagen en voorzien worden van een bewaartermijnclassificatie. Zodra de bewaartermijn is bereikt is worden deze documenten gewist.

Integriteit en vertrouwelijkheid
Lucas Onderwijs hanteert een clean desk policy. Daarnaast hebben medewerkers alleen toegang tot die persoonsgegevens die noodzakelijk zijn voor de uitvoering van hun taken. Er is een functiescheiding autorisatie. De Security Officer zegt hierover dat er wel wijzigingen van technische maatregelen doorgevoerd moeten worden voor medewerkers die toegang hebben tot systemen waar personeelsgegevens worden verwerkt doormiddel van een twee factor authenticatie of Multi factor authenticatie. Ten slotte maakt Lucas Onderwijs dagelijks back-ups van data zodat deze niet verloren gaan. Maandelijks back-ups worden tot een jaar terug bewaard.

3.2.3 Rechten van betrokkenen
Naleving van de wetgeving is de verantwoordelijkheid van het bestuur, maar naleving en borging hiervan kan alleen bereikt worden wanneer iedereen binnen Lucas onderwijs zorgvuldig en verantwoord met persoonsgegevens weet om te gaan. Om dit proces te ondersteunen wordt er vanuit het bestuur regelmatig gecommuniceerd d.m.v. presentaties, tips, flyer en nieuwsbrieven. Lucas Onderwijs heeft de rechten van betrokkenen opgenomen in een privacyverklaring. Lucas onderwijs heeft op intranet alles rondom de privacy en AVG gepubliceerd. Alle medewerkers hebben toegang tot deze informatie. Uit het interview met de HRM adviseur komt naar voren dat medewerkers niet expliciet worden gewezen op hun rechten. De gedachte hierachter is dat de rechten van medewerkers reeds bestonden voor de komst van de AVG.

Recht op inzage
Lucas Onderwijs heeft in 2018 met instemming van de MR alle personeelsdossiers gedigitaliseerd. Alle medewerkers zijn vooraf per e-mail geïnformeerd dat de personeelsdossiers worden gedigitaliseerd en hebben de mogelijkheid om bezwaar te maken. Sinds de digitalisering hebben de medewerkers inzage in hun personeelsdossiers en kunnen zijzelf eventuele wijzigingen doorvoeren. De invoering van de AVG heeft ertoe geleid dat medewerkers zelf in moeten loggen bij het pensioenfonds en dienen zij aldaar eventuele wijzigingen door te geven via de digitale portal.

Recht op rectificatie
Medewerkers hebben het recht op rectificatie. Het recht op rectificatie is voor Lucas Onderwijs vanzelfsprekend en wordt dus niet duidelijk gecommuniceerd. Medewerkers kunnen eventuele onjuistheden of aanvullingen zelf in hun personeelsdossiers doorvoeren. Persoonsgegevens waar zij zelf niet bij kunnen, zoals het Data Acces Managementsysteem kunnen zij doorgeven aan de beheerder.

Recht op vergetelheid
Een medewerker heeft het recht om Lucas Onderwijs te vragen om zijn persoonsgegevens te verwijderen indien de verwerking niet langer noodzakelijk is. Dit is bijvoorbeeld het geval als de wettelijke bewaartermijn is verstreken. Voor de gegevensverwerking van persoonsgegevens is het nog niet mogelijk om een bewaartermijn classificatie toe te kennen. Hierdoor kan niet altijd toegezien worden op de naleving van de wettelijke bewaartermijnen. Als een medewerker zich wil beroepen op het recht op vergetelheid is het belangrijk dat de medewerker op de hoogte is van deze gegevensverwerking.

Recht op beperking
Medewerkers hebben het recht om de verwerking van hun persoonsgegevens te beperken. Dit is het geval dat een verzoek tot rectificatie is gedaan of een medewerker bezwaar heeft gemaakt tegen de verwerking. Het ongevraagd verwerken van gegevens kan leiden tot situaties waarbij medewerkers bezwaar kunnen hebben tegen een verwerking.

Recht op dataportabiliteit
Dataportabiliteit is een nieuw recht wat medewerkers is toegekend en een medewerker mag alle opgeslagen en verwerkte bestanden opeisen om deze over te dragen aan zijn nieuwe werkgever. In de

privacyverklaring wordt het recht van dataportabiliteit niet genoemd. Lucas heeft de AVG op pragmatische wijze geimplementeerd.

3.2.4 DPIA en Datalekken

DPIA binnen de Lucas

Lucas Onderwijs dient een DPIA op te stellen bij een nieuwe vorm van persoonsgegevensverwerking. Dit is een taak van de Security Officer. Hiervoor gebruikt de Security Officer het DPIA-model van de leverancier Norea. In de DPIA worden de risico's in kaart gebracht en ook de maatregelen die genomen dienen te worden om deze risico's te vermijden.

Eventueel onaanvaardbare risico's worden met de verwerker besproken en wordt bekeken of deze risico's kunnen worden weggenomen of worden deze tot een aanvaardbaar niveau teruggebracht. Daarnaast wordt advies ingewonnen bij de AP over eventueel aanwezige risico's bij een nieuwe vorm van gegevensverwerking. De Security Officer vertelt dat de uitslag van de DPIA kan resulteren dat de aanschaf niet door kan gaan. Indien Lucas Onderwijs de intentie heeft om een softwarepakket of informatiesysteem aan te schaffen waarbij persoonsgegevens verwerkt worden dient de Security Officer binnen de Lucas onderwijs gevraagd worden om een DPIA op te stellen. De Security Officer heeft tot nu toe twee DPIA's uitgevoerd. De AVG-regiegroep geeft uiteindelijk uitsluitsel of het softwarepakket AVG-proof is en of het pakket aangeschaft kan worden. Indien er een discussie ontstaat dan dient het CvB een besluit te nemen en vraagt de Security Officer de verwerkersovereenkomst aan.

Datalekken

Lucas Onderwijs geeft via het intranet aanwijzingen hoe zij moeten handelen en hoe zij melding kunnen doen. Op het intranet zijn voorbeelden gegeven van datalekken. Alle medewerkers zijn verplicht om onmiddellijk melding te doen van een mogelijke datalek. De melding kan gedaan worden bij een direct leidinggevende of bij de Security Officer. De Security Officer onderzoekt de mogelijke datalek en neemt direct maatregelen ter voorkoming van verdere schade. De Security Officer meldt het incident bij de FG van Lucas Onderwijs. Op basis van de melding wordt aan de hand van de leidraad van de AP beslist of het incident gemeld moet worden bij de AP en of de betrokkenen al dan niet geïnformeerd moeten worden. De FG informeert het CvB. Uit het interview met de Security Officer blijkt dat sinds de invoering van de AVG zich twee incidenten van datalekken hebben voorgedaan. In beide gevallen is melding gedaan bij de AP. De Security Officer houdt een lijst van incidenten bij in een incidentenregister.

3.3 Conclusie

In dit hoofdstuk is antwoord gegevens op deelvragen 3 en 4. De onderzoeksmethoden en onderzoeksresultaten zijn hierin behandeld. Op basis van de documentenanalyse is naar voren gekomen dat Lucas Onderwijs vele inspanningen heeft verricht om de AVG te implementeren. De bewustwording van de organisatie en haar medewerkers en de benoeming van een FG zijn hier voorbeelden van. Ook zijn er afspraken vastgelegd en zijn er protocollen geïntroduceerd die in lijn zijn met de AVG. Uit de interviews is naar voren gekomen dat men bewust is van alle regels en richtlijnen met betrekking tot de AVG. Echter komt hier ook naar voren dat veel zaken als vanzelfsprekend worden beschouwd en de organisatie tekortschiet in enkele verplichtingen. Op het gebied van beginselen blijkt namelijk dat bij opslagbeperking documenten opgeslagen worden op de lokale schijf en in een mailbox blijven bestaan zonder dat wordt stilgestaan hoe lang deze documenten bewaard mogen worden. Het is momenteel niet mogelijk om een classificatie te maken in de bewaartermijnen. Ook vinden er gegevensverwerkingen plaats met overbodige informatie wat in strijd is met de minimale gegevensverwerking. Op het gebied van privacyrechten is recht op rectificatie niet duidelijk gecommuniceerd en is dit niet bekend bij medewerkers. Bij recht op vergetelheid wordt niet altijd toegezien op de naleving van de wettelijke bewaartermijnen aangezien het niet mogelijk is om een bewaartermijn classificatie toe te kennen. Het classificeren van de bewaartermijnen op korte termijn zou veel problemen dus kunnen verhelpen. Op het gebied van DPIA en datalekken staan op het intranet duidelijk aanwijzingen hoe gehandeld moet worden. De Security Officer is bovendien op de hoogte van alle verplichtingen en heeft inmiddels 2 DPIA's uitgevoerd.

4. Conclusies en Aanbevelingen

In dit hoofdstuk zijn de conclusies en aanbevelingen beschreven en wordt de centrale onderzoeksvraag beantwoord. De onderzoeksvraag luidt: “Wat moet er veranderen aan de huidige bedrijfsvoering van Lucas Onderwijs om te voldoen aan de AVG-richtlijn ten aanzien van de vaststelling en verwerking van personeelsgegevens?”

4.1 Conclusies

Na een intensieve documentenanalyse en interview met de Security Officer en de HRM adviseur, zijn de organisatorische inrichting, beginselen, rechten en personeelsdossierprocessen onder de loep genomen bij Lucas Onderwijs. Uit dit onderzoek is gebleken dat Lucas Onderwijs op de bekeken gebieden AVG Compliant is. Zij voldoen aan de harde eisen, maar er zijn ook enkele onbewuste tekortkomingen die tegenstrijdig zijn met de AVG.

Uit het onderzoek kan vastgesteld worden dat Lucas Onderwijs een jaar na de invoering van de AVG ten aanzien van de verwerking van personeelsgegevens op een aantal punten na voldoet aan de AVG. Als de aanbevelingen onder paragraaf 4.2 zijn opgevolgd kan gesteld worden dat Lucas Onderwijs volledig AVG-proof is ten aanzien van de verwerking van personeelsgegeven.

Lucas Onderwijs is in 2017 begonnen met het verkennen van de AVG-richtlijn en het inventariseren welke maatregelen genomen moeten worden om AVG-compliant te zijn. Er is gekozen voor een pragmatische aanpak waarbij de belangrijkste risico’s op datalekken de grootste aandacht hebben gehad. Lucas Onderwijs verwerkt op grote schaal bijzondere personeelsgegevens van haar leerlingen, ouders en verzorgers. Daarnaast deelt zij deze gegevens met instanties die de gegevens verwerken vanuit een publieke taak, zoals JGZ en de Gemeente. Bij de implementatie van de AVG hebben de gegevens van leerlingen, ouders en verzorgers de grootste aandacht gehad. Het is overduidelijk dat een mogelijke datalek van leerlinggegevens, ouders en verzorgers een hoog risico voor de rechten en vrijheden van deze betrokkenen met zich meebrengt.

Bij de invoering van de AVG zijn bijeenkomsten georganiseerd voor medewerkers en zijn presentaties gegeven over de AVG-richtlijn door de projectgroep AVG. Er is een flyer verspreid waarin instructies worden gegeven hoe omgegaan moet worden en is uitgelegd wat de definitie is van een datalek en hoe medewerkers moeten handelen bij een mogelijke datalek.

Lucas Onderwijs heeft een privacyverklaring opgesteld en heeft bestaande protocollen herzien. Daarnaast zijn nieuwe protocollen, en handreikingen gepubliceerd en via het intranet met de medewerkers gedeeld. Met verwerkers zijn nieuwe verwerkersovereenkomsten afgesloten en met verwerkers die tevens verwerkingsverantwoordelijke zijn, zijn privacy-convenanten afgesloten. Dit is gefaseerd gebeurd en is begonnen met verwerkers met een hoog risico.

Voor de gegevensverwerkingen wordt een dataregister bijgehouden. In het register worden de grondslagen en de doelen vermeld. Daarnaast is er een register van verwerkersovereenkomsten en datalekken bijgehouden. Bij een nieuwe vorm van gegevensverwerking wordt een DPIA uitgevoerd. Deze worden bewaard voor het geval de AP deze wil inzien en wil aan kunnen tonen hoe het besluit tot een nieuwe vorm van gegevensverwerking is genomen.

Lucas Onderwijs heeft technische maatregelen genomen om systemen beter te beveiligen tegen onbevoegde toegang tot verwerkingsapparatuur. Er is een functiescheiding autorisatie en computerapparatuur wordt automatisch vergrendeld als deze een bepaalde tijd niet wordt gebruikt. Wachtwoorden hebben een beperkte houdbaarheid. Systemen waar bijzondere gegevens worden verwerkt vereisen een dubbele authenticatie. Persoonsgegevens worden alleen uitgewisseld indien er een beveiligde verbinding is. Om te voorkomen dat gegevens verloren gaan of beschadigd raken wordt

regelmatig een back-up gemaakt. Deze worden tot een jaar terug bewaard. Om te zorgen dat systemen in geval van een storing opnieuw kunnen worden ingezet en de betrouwbaarheid en integriteit van systemen te kunnen waarborgen worden regelmatig updates geïnstalleerd.

Per 25 mei 2018 is de heer Y. Bleeker aangesteld als FG. Lucas onderwijs voldoet hiermee aan de verplichting van de AVG om een FG aan te stellen. De heer Y. Bleeker is oud-directeur van een middelbare school die onder het schoolbestuur van Lucas Onderwijs valt en heeft diverse managementfuncties bekleed. De heer Y. Bleeker heeft eerder de processen van de organisatie in beeld gebracht, hij is bekend met de organisatie en kan als deskundig worden gekwalificeerd. De heer Y. Bleeker is aangemeld bij de AP en zijn contactgegevens zijn op het intranet terug te vinden. De FG vervult geen andere functie binnen de organisatie en is autonoom ten aanzien van zijn taken.

Lucas Onderwijs heeft een protocol Datalekken gepubliceerd. In het protocol zijn de beleidsregels opgenomen hoe gehandeld moet worden bij een datalek en welke verplichtingen verwerkers is opgelegd die namens de organisaties persoonsgegevens verwerken. In het protocol staan tevens de contactgegevens van de Security Officer en de FG.

Lucas Onderwijs voldoet niet volledig aan het transparantie beginsel. Lucas Onderwijs heeft haar personeelsdossier gedigitaliseerd in Youforce en heeft haar medewerkers hierover geïnformeerd. Uit het interview met de HRM adviseur blijken niet alle personeelsdocumenten gedigitaliseerd. Dat betekent dat het zeer waarschijnlijk is dat sommige personeelsdossiers niet volledig zijn. De medewerkers om wie het gaat zijn bovendien niet hiervan op de hoogte gesteld. Een ander gegevensverwerking die plaatsvindt in organisatie die niet aan de transparantie, doelbinding en minimale gegevensbeginsel voldoet is de verwerking van personeelsgegevens in de rapportagetool Capisci. Medewerkers zijn niet op de hoogte dat zij in de rapportage tool voorkomen met hun salarisgegevens en er is ook geen toestemming gevraagd om dit deze gegevens te mogen verwerken. Bovendien leveren deze persoonsgegevens geen toegevoegde waarde aan een financiële rapportage, wat in strijd is met het beginsel van minimale gegevensverwerking. Uit het interview met de HRM adviseur blijken tevens intakeformulieren niet te zijn afgestemd op het beginsel van minimale gegevensbeginsel. Er wordt nieuwe medewerkers om gegevens gevraagd waarvan niet duidelijk is waar deze gegevens voor verwerkt worden.

De organisatie heeft gekozen om een Security Officer aan te stellen. De Security Officer heeft als voordeel dat de uitvoerende taken die de AVG met zich meebrengt bij deze functionaris ondergebracht kunnen worden. De Security Officer vervult tevens de functie van IT-beheer voor een aantal scholen. De Security Officer heeft hiermee twee functioneel leidinggevenden. De Security Officer ervaart hierdoor in bepaalde situaties een spanningsveld ten aanzien van zijn taken.

Binnen de organisatie worden op de financiële afdeling personele voorzieningen in de boekhouding verwerkt. In enkele gevallen betreft het vaststellingsovereenkomsten waarin met medewerkers is overeengekomen om de arbeidsovereenkomst te ontbinden waarbij medewerkers een transitievergoeding ontvangen. Uit het interview met de HRM adviseur komt daar voren dat de overeenkomsten per e-mail naar de afdeling Financiën & Administratie (F&A) worden verzonden. Volgens het beginsel van minimale gegevensverwerking moeten de gegevens beperkt zijn tot wat noodzakelijk is voor het doel waarvoor de gegevens verwerkt worden. Voor de financiële afdeling is de kostenplaats, het bedrag, kostenplaats en periode voldoende om een dergelijke personele voorziening in de boekhouding te registreren.

Het beginsel van opslagbeperking is wellicht een thema waar Lucas Onderwijs het minst zicht op heeft. De onmogelijkheden van systemen waarin persoonsgegevens worden verwerkt maken het lastig voor de organisatie om aan het beginsel van opslagbeperking te voldoen. De systemen die gebruikt worden hebben geen functies waarin documenten geclassificeerd kunnen worden in bewaartermijnen. Het gevolg hiervan is dat persoonsgegevens langer worden opgeslagen dan nodig is. Systemen waarin persoonsgegevens van medewerkers worden verwerkt zijn RAET, Youforce, Magister, Capisci en het

Document Management Systeem. Daarnaast worden documenten met persoonsgegevens van medewerkers per e-mail verzonden. Het is binnen de organisatie gebruikelijk dat e-mailberichten in de e-mailbox bewaard blijven waardoor niet toegezien kan worden op de bewaartermijn van de documenten met persoonsgegevens.

Uit de interviews blijkt verder dat medewerkers niet expliciet worden gewezen op hun rechten. Uit de interviews kan opgemerkt worden dat de rechten van medewerkers als vanzelfsprekend worden beschouwd omdat deze rechten al bestonden voor de invoering van de AVG. De AVG vindt dit echter niet voldoende. De AVG verplicht de verwerkingsverantwoordelijke om uitdrukkelijke toestemming te vragen aan haar medewerkers en mag de gegevens alleen verwerken voor het doel waar de gegevens voor verkregen zijn. Deels wordt voldaan aan de rechten van medewerkers. Het recht op inzage en rectificatie is ondervangen door het digitaliseren van de personeelsdossiers.

Het recht van dataportabiliteit is niet beschreven in het privacyreglement. Werknemers hebben het recht om hun dossier mee te nemen naar een nieuwe werkgever. De werkgever moet dit mogelijk maken. Daarom is het belangrijk dat de personeelsdossiers op orde zijn en geen onnodige informatie bevatten.

4.2 Aanbevelingen

Uit de conclusie is gebleken dat Lucas Onderwijs AVG Compliant gevonden kan worden indien enkele aanpassingen worden doorgevoerd. Deze worden hieronder uitgewerkt gevolgd door aanbevelingen die de positie van Lucas Onderwijs versterken op het gebied van Privacy.

Om aan het transparantiebeginsel te voldoen is het belangrijk om medewerkers te informeren dat het personeelsdossier niet volledig is. Bij het informeren dient tevens een termijn opgegeven te worden wanneer de oplevering zal plaatsvinden.

De personeelsgegevens in de rapportagetool Capisci zijn zonder toestemming van medewerkers opgenomen. De gegevens worden gebruikt voor een ander doel dan waar de gegevens voor zijn verzameld. Het is mogelijk om de gegevens zodanig te verwerken zonder dat deze aan een medewerker gekoppeld kunnen worden. Door de namen van medewerkers te vervangen door personeelsnummers is het alleen voor HRM-medewerkers mogelijk om te achterhalen om welke medewerkers het gaat.

Voor het registreren van personele voorzieningen in de boekhouding moet aan de minimale gegevensverwerking worden voldaan. In de huidige situatie worden vaststellingsovereenkomsten met persoonsgegevens doorgestuurd naar de afdeling Financiën. Behalve dat er meer gegevens worden meegegeven zullen deze overeenkomsten ook in de e-mailbox bewaard blijven waardoor niet toegezien kan worden op de opslagbeperking. Om aan de minimale gegevensverwerking te kunnen voldoen is het voldoende om het bedrag, afdeling, tijdvak en het personeelsnummer te verstrekken. Dit kan worden opgelost met een Excelformulier waarin deze gegevens worden ingevuld.

Het is belangrijk om na te gaan welke persoonsgegevens nodig zijn voor een gegevensverwerking. Het is belangrijk om het doel van elke gegevensverzameling te formuleren. Het formuleren van het doel helpt om te kunnen voldoen aan de minimale gegevensverwerking.

Om te kunnen voldoen aan het beginsel van minimale gegevensverwerking is het belangrijk dat de afdelingen HRM, PSA en Financiën afstemmen welke gegevens nodig zijn voor het registreren van personeelsvoorzieningen in de boekhouding. Hiermee wordt tevens deels aan het beginsel van opslagbeperking voldaan doordat documenten met persoonsgegevens niet meer in de e-mailbox bewaard hoeven te blijven.

In de huidige situatie is het niet mogelijk om in de systemen documenten te classificeren voor de bewaartermijn. Er is geen handreiking of protocol waarin beschreven is wat de bewaartermijnen zijn. Uit

beide interviews wordt geantwoord dat de organisatie de wettelijke bewaartermijn hanteert. De Security Officer heeft een overzicht van bewaartermijnen maar wordt niet gedeeld in de organisatie. Het is aan te bevelen om een beleidsdocument op te stellen waarin de bewaartermijnen worden vastgesteld. Dit zorgt voor een uniforme werkwijze en schept duidelijkheid bij alle medewerkers.

Er dienen regels opgesteld te worden voor de opslag van persoonsgegevens, waarin beschreven wordt waar deze opgeslagen dienen te worden en hoe om te gaan met e-mailberichten waarin persoonsgegevens zijn opgenomen. Het is mogelijk om per e-mail met een link te verwijzen naar opgeslagen documenten in het DMS. Op deze manier hoeven documenten met persoonsgegevens niet als bijlagen verzonden te worden. Door de optie voor het downloaden van documenten uit het DMS uit te schakelen wordt afgedwongen dat medewerkers gebruik maken van de verwijzing naar het DMS.

Leveranciers moeten betrokken worden om een oplossing te vinden om te kunnen voldoen aan het beginsel van opslagbeperking. Door de wensen aan de leveranciers kenbaar te maken kunnen leveranciers deze aanpassingen doorvoeren en kunnen deze verbeteringen door updates worden opgelost.

Aangezien de huidige systemen niet in een bewaartermijn classificatie voorzien is het aan te bevelen dat deze eis wordt opgenomen in de format “Programma van Eisen” en tevens in het DPIA-model wat gebruikt wordt om ervoor te zorgen dat systemen waar in de toekomst gebruik van gemaakt zal worden voldoen aan deze eis.

De Security Officer heeft in tegenstelling tot de FG geen ontslagbescherming ten aanzien van zijn taken. Zijn taken als IT-beheerder en Security Officer levert soms een spanningsveld op vanwege de tegenstrijdige belangen omdat hij met twee functioneel leidinggevenden te maken heeft. Het is wenselijk om de Security Officer anders te positioneren binnen de organisatie. Dit kan opgelost worden door de stichtingsdirecteur functioneel leidinggevende te maken voor de Security Officer. Dit biedt de Security Officer bescherming ten aanzien van zijn taken voor de AVG.

Het recht op dataportabiliteit is niet benoemd in de privacyverklaring. Het dient aan te bevelen om dit recht op te nemen in de privacyverklaring. Het is belangrijk dat personeelsdossiers juist en volledig zijn en geen irrelevante documenten bevatten. Bovendien moet dit in een gangbaar bestandformaat geleverd worden.

5. Nawoord

Bij de start van mijn scriptie was ik erg gemotiveerd. Ik was erg ambitieus maar niet realistisch met mijn planning. Ik heb geleerd dat een goede planning en afbakening zeer belangrijk is. Tijdens het onderzoek naar de AVG-richtlijn en de Wbp heb ik veel geleerd. Het onderzoek heeft mij privacy bewust gemaakt. Zowel in de privé situatie als op het werk kijk ik kritisch naar privacygevoelige informatie.

Door de slechte planning, de vele ballen die ik moet hooghouden, heb ik een achterstand opgebouwd. De achterstand heb ik in korte tijd weten in te halen. De laatste stappen zijn nu gezet. Ik ben tevreden met het resultaat.

5.1 Taakreflectie

Literatuuronderzoek
Het theoretisch kader was een uitdaging. De Wbp bood genoeg artikelen, literatuur en praktijkvoorbeelden. De AVG daarentegen is een vrij nieuw onderwerp waardoor er beperkte informatiebronnen te vinden waren. Bij het onderzoeken van deze privacywet is hierdoor voornamelijk gebruik gemaakt van de wetsartikelen en handleidingen van het AP. Uit de hoeveelheid ruwe informatie heb ik een logische opbouw weten te maken in bruikbare literatuur die uiteindelijk antwoord geven op mijn deelvragen (zonder de vragen voor het veldonderzoek). Na deze logische opbouw aan informatie en het visueel schetsen in een model is er voldoende draagvlak gecreëerd voor het uitvoeren van een empirisch onderzoek. Het onderzoek kon meer literatuuronderzoek gebruiken, maar gezien de beperkte bronnen en de lage generaliseerbaarheid van andere literatuurbronnen was dit geen optie.

Gehanteerde onderzoeksmethodologie
Om te komen tot mijn onderzoeksmethodologie heb ik gebruik gemaakt van het boek Business Research Methods van Boris Blumberg en Research Methods for Business Students van Saunders, Lewis en Thornhill. Bij het afsluiten van mijn literatuuronderzoek had ik vragen waar ik antwoord op wilde. Ik wist dat ik enkele vragen al kon beantwoorden aan de hand van documenten waar ik toegang toe kon krijgen. Er zaten ook vragen tussen waar dit niet mogelijk was en ik iemand moest spreken die mij meer kon vertellen over de organisatie op het gebied van AVG. Zo kwam ik met het boek tot de conclusie dat een Documentenanalyse en een Semi-Gestructureerd interview, ofwel een Case Study, het antwoord zou geven op mijn vragen. Ik heb de geïnterviewden, de Security Officer en een HRM Adviseur gevraagd om een interview af te mogen nemen en daar werd heel positief op gereageerd waardoor ik na enkele dagen met hen aan tafel zat.

Voorafgaand aan het interview heb ik de vragenlijst opgesteld, en deze heb ik kritisch na laten kijken om goede resultaten te verkrijgen. Bij het verzamelen van de data kwam ik erachter dat een semigestructureerd interview meer skills vereist om het gesprek te sturen in de juiste richting. Een interview loopt uit en informatie wordt verzameld wat niet altijd relevant is. Bij het transcriberen van het interview kwam ik hier voornamelijk achter. Hier heb ik in het 2e gesprek rekening mee gehouden door over te gaan naar de volgende vraag op het moment dat het een “gezellig gesprek” begon te worden.

Er heeft geen interview met een verwerker plaatsgevonden. Aangezien verwerkers degene zijn die daadwerkelijk met de persoonsgegevens werken, hadden de resultaten betrouwbaarder kunnen zijn als ik ook een verwerker had geïnterviewd. Hiermee had ik de praktijk bij Lucas Onderwijs kunnen toetsen aan de verkregen antwoorden uit het interview met de HRM adviseur en Security Officer.

Onderzoeksuitkomsten
Bij het uitwerken van de documentenanalyse en interviews is belangrijke informatie gefilterd om niet overspoeld te raken met (onbruikbare) informatie. Deze zijn zodanig vastgelegd dat zij beschrijvend antwoord geven op de vragen. Hieruit bleek dat Lucas Onderwijs (onbewust) niet voldoet aan alle eisen. Dit bood voldoende inzichten en gronden om aanbevelingen te doen naar Lucas Onderwijs.

Mijn verwachtingen komen vrij overeen met mijn eerdere veronderstellingen. Aangezien ik werkzaam ben bij Lucas Onderwijs ken ik de manier van werken en weet ik (ongeveer) waar de tekortkomingen liggen. Hierdoor zijn de resultaten niet verrassend geweest. Ik vermeld hier tevens bij dat ik Lucas Onderwijs heb onderschat in de genomen maatregelen voor de AVG aangezien veel gebeurde achter de schermen.

Voor het uitvoeren van het praktisch onderzoek is er eerst een empirisch model gemaakt wat gebaseerd is op literatuur. Dit model is in de praktijk getoetst aan Lucas Onderwijs en de resultaten zijn in die volgorde uitgewerkt, waardoor de rode draad in het onderzoek zichtbaar is gebleven in heel het rapport.

5.2 Zelfreflectie

Hieronder beschrijf ik mijn ervaringen tijdens het onderzoek bij Lucas Onderwijs. Dit heb ik gedaan aan de hand van de STARR-methode.

1. Wat was de situatie?

Ter aanvulling op de documentanalyse heb ik in juli twee semi-gestructureerde interviews gehouden om de processen compleet te maken. De vragen waren gericht op de privacy van personeelsgegevens. Er is ruimte gelaten voor AVG in het algemeen omdat de personeelsgegevens maar een klein deel vormen van alle gegevensverwerkingen in de organisatie. Dit heeft extra informatie opgeleverd die in het onderzoek betrokken kon worden. Voor het onderzoek heb ik de HRM adviseur en de Security geïnterviewd.

2. Wat was je taak?

Tijdens het interview had ik de rol van interviewer om vragen te stellen. Het doel van het interview was om de ontbrekende informatie uit het documentenonderzoek aan te vullen en mogelijk nieuwe bruikbare informatie te verkrijgen. De verwachting van de HRM adviseur was dat ik vragen stel die gericht waren op de HRM-processen en voor de Security Officer op de uitvoering en toezicht op de AVG-organisatie. Tijden het interview verwachtte ik van mijzelf om goed te luisteren en te herhalen wat gezegd wordt om eventueel door te kunnen vragen. De vragen waren kritisch en deden soms de Security Officer tot nadenken.

3. Hoe heb je het aangepakt en waarom?

Tijdens het beschrijven van de AVG-organisatie aan de hand van het documentenonderzoek heb ik daarnaast een vragenlijst voor de HRM adviseur en de Security Officer bijgehouden. Alles wat niet uit documenten beantwoord kon worden heb ik als vraag opgeschreven. Nadat ik klaar was met de documentanalyse heb ik de vragen verbeterd en verder aangepast en hier open vragen van gemaakt.

4. Heeft het gewerkt en waarom?

Op papier kan de organisatie AVG-compliant zijn, maar in de praktijk hoeft dat niet zo te zijn. Het interview is dus essentieel en heeft bruikbare informatie opgeleverd. Het grootste gedeelte van de aanbevelingen is gebaseerd op de uitkomsten van de interviews.

5. Wat heb je ervan geleerd?

Als ik terugkijk op de interviews dan ben ik tevreden met hoe het is gegaan. De vragen waren goed en ik haakte in op antwoorden waar mogelijke meer informatie achter zou kunnen zitten. Na het verwerken van de interviews kwam ik toch tot de conclusie dat ik bepaalde vragen niet heb gesteld die mogelijk meer informatie hadden kunnen opleveren. Alle onderdelen van een onderzoek vormen samen het onderzoeksrapport. Het interview mag hier niet ontbreken omdat deze een schat aan informatie oplevert. Ik heb met toestemming de gesprekken opgenomen zodat ik tijdens het uitwerken dit kan terugluisteren. Daar ben ik achteraf heel blij mee. Bij het terugluisteren van de interviews betrap ik mijzelf erop dat ik zinnen probeer af te maken terwijl zij aan het woord zijn. Dat ervaar ik zelf als storend en daarmee beïnvloed ik ook mogelijk het antwoord. Dat moet ik de volgende keer anders doen. Deze ervaring neem ik uiteraard mee en zal ik toepassen in nieuwe situaties die zich voordoen.

Literatuurlijst

Algemene Verordening Gegevensbescherming. (2016, 6 april). Geraadpleegd op 1 mei 2019, van https://www.pmpartners.nl/wp-content/uploads/2016/04/CONSIL_ST_5419_2016_INIT_NL_TXT-1.pdf

Autoriteit Persoonsgegevens. (2018, 6 februari) Guidelines meldplicht datalekken. Geraadpleegd op 6 juli 2019, van https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht_datalekken.pdf

Autoriteit Persoonsgegevens. (z.j.). In 10 stappen voorbereid op de AVG. Geraadpleegd op 22 juli 2019, van https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/in_10_stappen_voorbereid_op_de_avg.pdf

Autoriteit Persoonsgegevens. (2017, 4 april). Richtsnoeren voor gegevensbeschermingseffectbeoordelingen. Geraadpleegd op 25 juli 2019, van https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp248_rev.01_nl.pdf

Autoriteit Persoonsgegevens. (2017, 4 april). Rechten van betrokkenen. Geraadpleegd op 24 juli 2019, van https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp260rev01_nl.pdf

Autoriteit Persoonsgegevens.(z.j.) Richtlijnen FG. Geraadpleegd op 27 april 2019, van https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtlijnen_fg.pdf

Blumberg, B., Cooper, D. R., & Schindler, P. S. (2008). *Business research methods* (Vol. 2). London: McGraw-Hill Higher Education.

De IT-jurist. (2017, 20 februari). Het recht op overdraagbaarheid van gegevens. Geraadpleegd op 23 juli 2019, van https://www.it-jurist.nl/nieuws/het-recht-op-overdraagbaarheid-van-gegevens

De Vries, H. H. (2010). Evaluatie en toekomst van de Wet bescherming persoonsgegevens.

Kennisnet. (2018, 30 april). Handreiking Functionaris gegevens bescherming. Geraadpleegd op 26 april 2019, van https://www.kennisnet.nl/fileadmin/kennisnet/informatiebeveiliging-privacy-ibp/Bestanden/Kennisnet-Handreiking-functionaris-gegevensbescherming.pdf

Kroeks-de, R. C., Westerdijk, R. J. J., & Zwenne, G. J. (2016). De Algemene Verordening Gegevensbescherming. Tijdschrift voor Internetrecht, 2016, 9.

Memorie van toelichting. (1998, 2 maart). Geraadpleegd op 2 januari 2019, van https://zoek.officielebekendmakingen.nl/kst-25892-3.html

Privacyconvenant onderwijs. (2018, maart) Model verwerkingsovereenkomst 3.0. Geraadpleegd op 18 juli 2019, van https://www.privacyconvenant.nl/het-convenant

Saunders, M., Lewis, P., & Thornhill, A. (2009). Research Methods for Business Students (5 ed.). New Jersey, United States: Prentice Hall.

Schoolenberg, M. (2019, 16 juli). fikse-boete-voor-haga-ziekenhuis-om-gluren-dossier-barbie. Geraadpleegd op 20 juli 2019, van https://www.telegraaf.nl/cookiewall?returnTo=/nieuws/1067370344/fikse-boete-voor-haga-ziekenhuis-om-gluren-dossier-barbie

Snijder, J., & de Groot, R. (2018, 12 april). De basisbeginselen van de Algemene Verordening Gegevensbescherming. Geraadpleegd op 18 september 2019, van https://www.wijnenstael.nl/nieuws/2018/de-basisbeginselen-van-de-algemene-verordening-gegevensbescherming

Swaen, B. (2014, 19 september). Validiteit van scriptieonderzoek. Geraadpleegd op 14 september 2019, van https://www.scribbr.nl/onderzoeksmethoden/validiteit-van-scriptieonderzoek/

Vermissen, K., Terstegge, J., & Krijgsman, N. (2017). *Grip op de AVG*. Deventer, Nederland: Wolters Kluwer.

Vleeshouwers, L. (2017, 1 augustus). steekproef in je scriptie. Geraadpleegd op 14 september 2019, van https://www.scribbr.nl/onderzoeksmethoden/steekproef-in-je-scriptie/

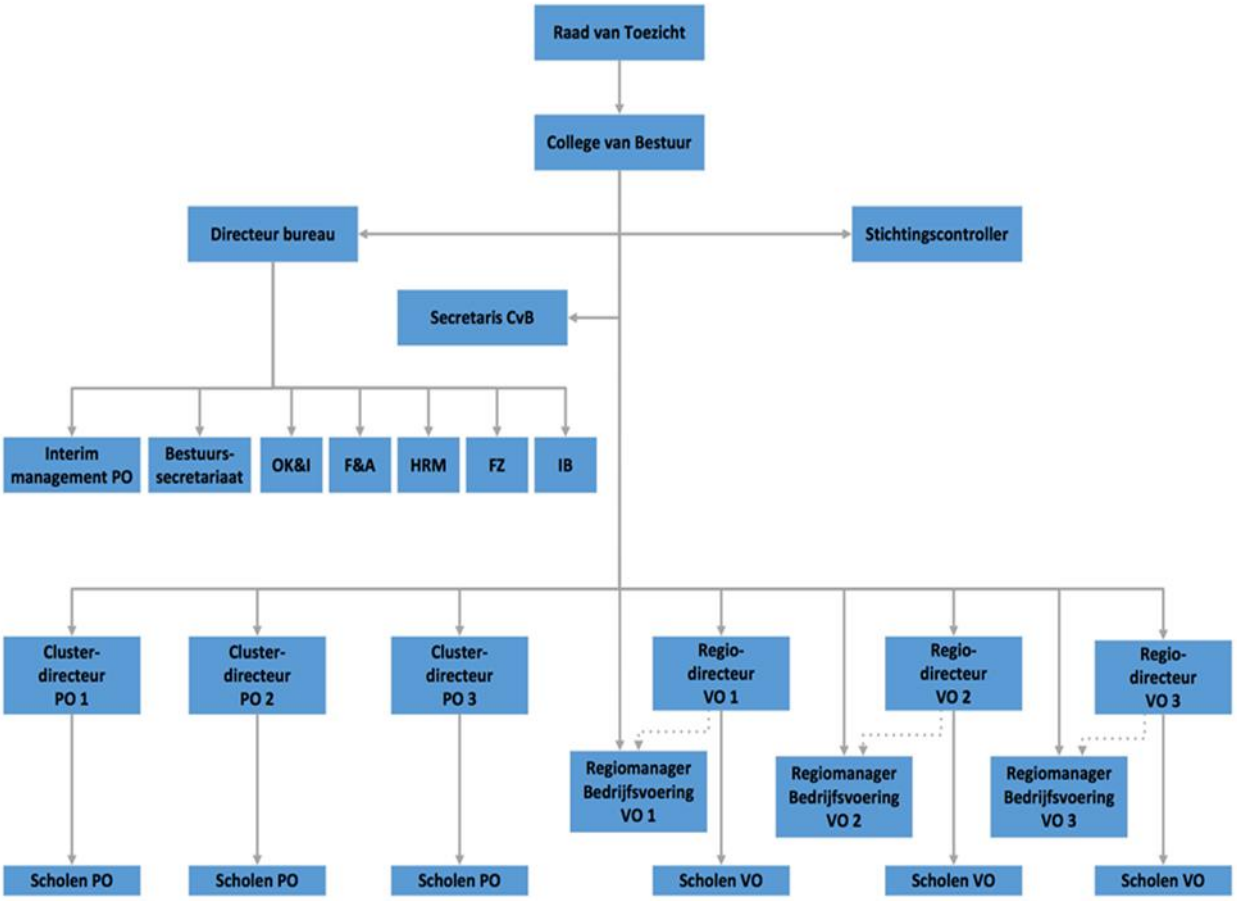
Wet Bescherming Persoonsgegevens. (2000, 6 juli). Geraadpleegd op 27 april 2019, van https://wetten.overheid.nl/BWBR0011468/2018-05-01

Wetboek van Strafrecht. (1881, 3 maart). Geraadpleegd op 27 april 2019, van https://wetten.overheid.nl/BWBR0001854/2019-04-01

Winter, H. B., De Jong, P. O., Sibma, A., Visser, F. W., Herweijer, M., Klingenberg, A. M., & Prakken, H. (2008). Wat niet weet, wat niet deert: een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk.

Zwenne, G. J., & Mommers, L. (2016). De tien belangrijkste veranderingen die de Algemene Verordening Gegevensbescherming gaat brengen. Tijdschrift voor Compliance, 2016, 8.

Bijlage 1: Organogram Stichting Lucas Onderwijs



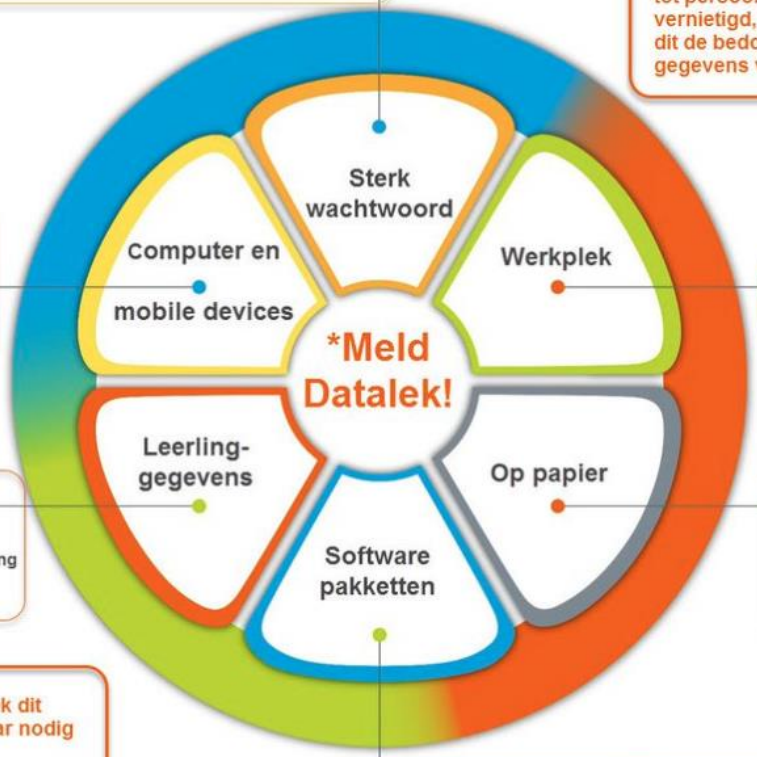
Hoe omgaan met persoonsgegevens

Voorkom datalekken!

Lucas Onderwijs hanteert de algemene beveiligingsregels die zoveel als mogelijke softwarematig wordt afgedwongen. Hierbij moet gedacht worden aan:
- Regelmatig moet het wachtwoord afhankelijk van de applicatie aangepast worden
- Controle op wachtwoord (mag voor een bepaalde periode niet dezelfde letter/cijfer reeks gebruiken)
- Na een aantal keren foutief invoeren wordt de toegang geblokkeerd
- Het wachtwoord moet een sterk wachtwoord zijn met letters, cijfers en symbolen. Gebruik geen namen, geboortedata of adressen.

Wanneer is er sprake van een Datalek

We spreken van een datalek als er onrechtmatig toegang is tot persoonsgegevens of als persoonsgegevens zijn vernietigd, gewijzigd, verloren of vrijgekomen, zonder dat dit de bedoeling is. Ook het onrechtmatig verstrekken van gegevens valt daaronder.



Advies:
- Beeldscherm vergrendelen zodra je je plek verlaat (Windows/L toets) L
- Alle mobile devices versleutelen met toegangscode
- Versleutel ook altijd je USB-stick
- Mail versturen met E-mailadressen in BCC

Advies:
Laat geen papieren met vertrouwelijke gegevens of wachtwoorden liggen op je werkplek

Je mag geen leerling gegevens delen bijv.:
- Geen klassenlijsten met n.a.w. gegevens e.d. verspreiden zonder toestemming
- Geen foto's of video's plaatsen zonder (jaarlijkse) toestemming
- Geen leerlinggegevens mailen of opslaan in "eigen" cloud omgeving of op "eigen" media (bijv. usb-stick)

Advies:
- Leg dossiers altijd op de juiste plaats terug
- Houd dossiers niet onnodig bij je
- Vernietig kopieën als ze niet meer nodig zijn
- Haal direct na printen van vertrouwelijke gegevens de kopieën weg bij het apparaat en/of print beveiligd

*Meld bij twijfel over een mogelijk datalek dit direct aan de directie. Deze kan dan waar nodig de benodigde stappen ondernemen.

Let op: Niet het datalek zelf is strafbaar maar het niet melden!

Lucas Onderwijs is verplicht om met leveranciers van softwarepakketten waarin verwerking van privacy gevoelige gegevens plaatsvindt een "Bewerkersovereenkomst" af te sluiten. Op de site <https://www.privacyconvenant.nl/de-deelnemers> is terug te vinden welke leveranciers al zo'n overeenkomst hebben ondertekend. Check deze lijst voordat je een nieuw softwarepakket gaat gebruiken. Mocht de naam van de leverancier hier niet op voorkomen geef dit dan door aan de directie. Zij zullen het bestuur dan op de hoogte brengen.

Bijlage 3: Randvoorwaarden en interviewvragen

Randvoorwaarden:

- De plaats van het interview bij Lucas Onderwijs zelf in een ruimte waar zo min mogelijk gestoord kan worden.
- De zitplaats vormen in een hoek van 90 graden om weg te kijken om niet onrustig over te komen.
- Aangeven aan respondent dat het interview 1 uur gaat duren
- Toestemming vragen om de naam te gebruiken in het onderzoek
- De achtergrond van het onderzoek en de toegevoegde waarde toelichten van het interview
- De respondent vertellen dat zij mag onderbreken voor vragen of verduidelijking
- De te stellen vragen moeten duidelijk zijn, en vriendelijk in de formuleringen zodat het gevoel niet wordt gegeven dat zij zichzelf moeten verdedigen.
- Anticiperen op non-verbale signalen zoals afwezigheid of zenuwachtigheid door de respondent met zijn volledige aandacht terug bij het interview te betrekken.
- Doorvragen bij de respondent bij omslachtige antwoorden of een vraag ter controle stellen.
- Tussendoor controleren of de opname nog loopt
- De respondent meer laten praten dan dat de interviewer praat
- Concluderend samenvatten na elke topic

Vragenlijst Interview HRM Adviseur

1. Hoeveel medewerkers zijn werkzaam bij Lucas Onderwijs?
2. Hoeveel mensen werken op de HRM en PSA-afdeling?
3. Is de HRM zich bewust van de nieuwe AVG? Zo ja waar blijkt dit uit?
4. Welke wijzigingen heeft HRM doorgevoerd bij de invoering van de AVG?
5. Heeft HRM wijzigingen in processen moeten aanbrengen om AVG-compliant te zijn?
6. Welke systemen worden gebruikt bij de geautomatiseerde verwerking van de (bijzondere) gegevens van personeelsleden?
7. Kan je het proces beschrijven van een solliciterende/ in dienst/ uit dienst tredende medewerker?
8. Kan je het proces beschrijven van een ziekteverzuim en Arbo?
9. Wordt (nieuwe) medewerkers gevraagd om toestemming om hun personeelsgegevens te mogen verwerken? (Transparantiebeginsel)?
10. Wordt (nieuwe) medewerkers gewezen op hun rechten t.a.v. de AVG?
11. Worden medewerkers geïnformeerd hoe lang persoonsgegevens worden opgeslagen?
12. Welke bewaartermijnen worden gehanteerd op de afdeling HRM PSA?
13. Hoe is de toegang tot personeelsbestanden geregeld?
14. Wordt de output van de gegevensverwerking doorgegeven aan andere afdelingen binnen de organisatie?

Vragenlijst Interview Security Officer

1. Is de organisatie zich bewust van de AVG?
2. Is de organisatie bewust van de rollen verwerker en verwekingsverantwoordelijke?
3. Is een FG verplicht voor Lucas onderwijs?
4. Wat zijn binnen Lucas onderwijs de taken van de FG?
5. Is er een Security Officer werkzaam binnen Lucas onderwijs, zo ja, wat zijn de werkzaamheden?
6. Waarom heeft Lucas onderwijs een Security Officer aangesteld?
7. Wat zijn de taken van de Security Officer?
8. Wordt er een verwerkingsregister bijgehouden van de verwerking van persoonsgegevens? Zo ja, wie houdt deze bij?
9. Zijn alle verwerkingsovereenkomsten met derden herzien bij de invoering van de AVG?
10. Zijn alle verwerkingsovereenkomsten nu toereikend en voldoen deze aan de vereisten in de AVG?

11. Welke wijzigingen zijn er aangebracht in het gegevensverwerkingsproces toen de AVG werd ingevoerd?
12. Hoe heeft Lucas Onderwijs haar activiteiten georganiseerd met betrekking tot beginselen van de AVG?
13. Worden personeelsleden geïnformeerd over hun rechten?
14. Wordt betrokkene geïnformeerd over de eventuele verwerking van haar of zijn persoonsgegevens en voor welk doel?
15. Hoe past Lucas onderwijs het beginsel van minimale gegevensverwerking toe?
16. Wat is het beleid op de bewaartermijn voor de opslag van persoonsgegevens?
17. Welke maatregelen heeft Lucas onderwijs genomen om persoonsgegevens te beveiligen tegen ongeoorloofd toegang of onrechtmatige verwerking?
18. Wordt medewerkers gevraagd om toestemming voor de verwerking van hun gegevens? en hoe wordt dit gedaan?
19. Informeert Lucas Onderwijs haar medewerkers over hun privacyrechten ten aanzien van de verwerking van hun persoonsgegevens? Zo ja, hoe worden zij geïnformeerd?
20. Is een DPIA verplicht voor Lucas Onderwijs?
21. Voert Lucas Onderwijs een DPIA uit? En zo ja wie voert dit uit?
22. Welke maatregelen zijn er genomen om datalekken te voorkomen?
23. Wordt er overleg gepleegd met de AP indien risico's niet gedekt kunnen worden?
24. Welke maatregelen worden genomen op het moment dat een risico niet gedekt kan worden?
25. Heeft Lucas onderwijs een PIA uitgevoerd? Wat zijn de uitkomsten hiervan als het gaat om de verwerking van persoonsgegevens van personeelsleden?
26. Is de bewaartermijn ergens vastgelegd in de organisatie?
27. Is er ook een PDCA-check?

Bijlage 4: Interview HRM adviseur

Hoeveel medewerkers zijn werkzaam bij Lucas Onderwijs?
Ik denk dat het ongeveer 3.000 FTE zijn. We hebben heel veel parttime medewerkers, dus ik weet niet zo precies hoeveel medewerkers bij Lucas werken.

Hoeveel mensen werken op de HRM en PSA-afdeling?
Op de afdeling HRM en PSA samen werken ongeveer 30 medewerkers. Dit zijn personeelsadviseurs, juridisch adviseurs en de salarisadministratie.

Is de HRM zich bewust van de nieuwe AVG? Zo ja waar blijkt dit uit?
We weten dat het speelt, maar dat is een andere vraag dan doe je het altijd goed. Het maakt het werk niet altijd makkelijk. Ik moet op een andere manier aan mijn gegevens komen. Als afdeling HRM en PSA is het belangrijk dat wij zorgvuldig omgaan met de privacy van personeelsleden.

Welke wijzigingen heeft HRM doorgevoerd bij de invoering van de AVG?
Sinds de invoering van de AVG mag het BSN-nummer niet meer vermeld worden. Formulieren zijn hierop aangepast. Het verzuimdossier mag geen BSN-nummer verwerken maar de arbodienst heeft wel het BSN-nummer nodig. Nu moet ik een kopie maken van het paspoort zonder het BSN-nummer maar heb ik juist het BSN-nummer nodig. We hebben dit nu overboord gegooid en gebruiken een kopie van het paspoort met het BSN-nummer. Sinds de komst van de AVG is de inrichting van systemen veranderd.

We merken dat bijvoorbeeld met sollicitaties, je mag niet zomaar meer gegevens doorspelen van sollicitanten. Het heeft altijd wel in de sollicitatiecode gestaan dat je toestemming moet vragen en dat het een jaar in portefeuille gehouden mag worden.
Door de AVG is het allemaal strenger geworden en zullen mensen waarschijnlijk eerder geneigd zijn om nee te zeggen.

Sinds de invoering van de AVG kunnen personeelsleden zelf inloggen in hun digitaal dossier Youforce en eventuele wijzigingen doorvoeren. Mensen moeten nu veel meer zelf doen, dat gaat nu niet meer via ons. Vroeger kon ik bijvoorbeeld een pensioenadvies opvragen bij ABP voor een medewerker. Dat mag ik nu niet meer, ik mag het ook niet inzien. Ik mag ook niets opslaan wat ik niet van de medewerker zelf ontvangen heb.
Een medeweker heeft zelf de keus om het wel of niet aan te leveren bij een personeelsadviseur. Het kan zijn dat natuurlijk altijd zo hoorde maar zo ging het niet. Het is nu vastgelegd dat iets niet mag. Voorheen kreeg mondeling toestemming om iets voor een medewerker op te vragen maar dat kan niet meer. De security officer heeft ook aangegeven dat de AVG in de regels niet eens zoveel heeft veranderd maar in de praktijk dus wel.

Heeft HRM-wijzigingen in processen moeten aanbrengen om AVG-compliant te zijn? Processen zijn anders. Voorheen kon in voor een medewerker een WIA aanvragen. Door de invoering van de AVG moet een medewerker dat zelf aanvragen middels zijn digiD. Ik mag het zelf niet meer doen. De persoon moet nu naast mij zitten en dan geef ik aanwijzingen waar hij wat moet aanklikken.

Welke systemen worden gebruikt bij de geautomatiseerde verwerking van de (bijzondere) gegevens van personeelsleden?
RAET voert de salarisverwerking van Lucas onderwijs uit. RAET heeft tevens een digitaal portaal waar Lucas Onderwijs gebruik van maakt voor HR- en personeelszaken. Het digitaal portaal heet Youforce. Hierin kunnen medewerkers inloggen om bij hun dossier te kunnen waarin alle documenten staan opgeslagen.

De verzuimregistratie verloopt ook via Youforce. Dit heet verzuimmanager. Verzuimmanager staat gekoppeld met het systeem van de Arbodienst Zorg van de Zaak. Zorg van de Zaak krijgt een melding vanuit verzuimmanager wanneer een medewerker 4 weken ziek is. Zorg van de Zaak nodigt de medewerker uit voor een gesprek. Als wij willen dat een medewerker eerder wordt uitgenodigd door Zorg van de Zaak dan sturen wij een emailbericht naar Zorg van de Zaak met naam en geboortedatum en het verzoek om de medewerker uit te nodigen. In het verzoek worden de relevante vragen aan de bedrijfsarts gesteld. Zorg van de Zaak vraagt dan om een BSN-nummer en die hebben we natuurlijk niet. Je mag een leidinggevende uit vrije wil vertellen wat je hebt maar je leidinggevende mag het niet vastleggen. Je leidinggevende mag er ook niet naar vragen.

Wij gebruiken ook het systeem Foleta. Dit wordt gebruikt voor de lesplanning tegelijkertijd gebruik ik het om te kijken of de scholen zich houden aan de begrotingsnorm.
Wij hebben daarnaast nog rapportage en begrotingssysteem Capisci waar ook persoonsgegevens van medewerkers in staan en we communiceren ook veel per email.
HRM werkt niet met het Document Managenet systeem M-files. Wij zouden een eigen kluis in M-files moeten hebben.

Voor het UWV is er een werkgeversportal waarin wij inloggen en gegevens opgeven en ophalen.
Er komt een overeenkomst met een drietal uitzendbureaus die medewerkers leveren voor Lucas Onderwijs. Er komt een platform waarin wij vacatures voor tijdelijke detachering kunnen plaatsen en waar de uitzendbureaus cv's van mensen aan kunnen koppelen. Dit is voor invulling voor tijdelijke vacature's

Kan je in het proces beschrijven van een solliciterende/ in dienst tredende medewerker?

Nieuwe medewerker in dient/ uit dienst

1. Vacature
2. Uitnodiging gesprek
3. Medewerker in dienst
4. Gegevens invoeren in Youforce door afdeling
5. HRM controleert gegeven in Youforce,
6. Salarisadministratie controleert gegevens in Youforce
7. Salarisadministratie stuurt een link per email aanvraag VOG verklaring
8. Alle benodigde documenten controleren op volledigheid
9. Akte van benoeming volgt per mail.

Ziekteverzuim en Arbo

1. Ziekmelding bij de leidinggevende
2. Leidinggevende voert melding in verzuimmanager
3. Traject loopt
4. Na 5 weken automatische uitnodiging van de bedrijfsarts Zorg van de Zaak.

In sommige gevallen kan je al bij de eerste ziektedag een medewerker door de bedrijfsarts laten uitnodigen. De bedrijfsarts legt alles vast in hun eigen systeem dat in verbinding staat met verzuimmanager. De bedrijfsarts deelt alleen de relevante informatie met ons.

Medewerker uit dient

1. Medewerker uit dienst verloopt via youforce
2. Mutatieformulier medewerker uit dienst
3. Reden uit dienst
4. Eventuele transitievergoeding
5. Of ziek uit dienst
6. Medewerkers moeten zelf een WW aanvragen

Wordt (nieuwe) medewerkers gevraagd om toestemming om hun personeelsgegevens te mogen verwerken? (Transparantiebeginsel)
Wij vragen nieuwe medewerkers geen toestemming voor de verwerking van hun persoonsgegevens. Er zijn soms wel vragen die nieuwe medewerkers gesteld worden waarbij je je kan afvragen in hoeverre deze gegevens relevant zijn. Een bijzondere vraag die gesteld wordt is heeft u een partner en zo ja wat zijn de gegevens van je partner. Mensen zijn nog wel bereid om te zeggen dat ze een partner hebben maar ik heb een aantal keren meegemaakt dat mensen zeggen dat gaat u helemaal niets aan wat de geboortedatum van mijn partner is. Ik heb nagevraagd waarom wij de geboortedatum van een partner nodig hebben maar daar kan niemand antwoord opgeven. Voor het pensioenfonds is het voldoende om te melden dat een medewerker een partner heeft. Dus wij hebben nu afgesproken dat op het moment iemand daar geen antwoord op wil geven dan vermelden we bij de geboortedatum onbekend. Je kunt tegenwoordig ook bij geslacht opgeven onbekend. Ik denk waarom zou iemand niet willen zeggen of hij een man of vrouw is maar dat recht hebben ze. Maar wordt het standaard gevraagd. Ik denk het niet. Het feit dat je het aanlevert stem je eigenlijk in dat wij de gegevens mogen verwerken.

Wordt (nieuwe) medewerkers gewezen op hun rechten t.a.v. de AVG?
Jawel, Toen het personeelsdossier is gedigitaliseerd heeft iedereen een email gekregen dat dit staat te gebeuren en als iemand bezwaar heeft dan kon je dat melden en iedereen weet dat je inzage hebt in je personeelsdossier. Personeelsleden hadden voor de invoering van de AVG al het recht van inzage van hun gegevens en als gegevens niet actueel zijn dan kunnen ze verzoeken om de gegevens aan te passen. Personeelsleden hebben nu toegang tot hun. Wij hebben alle Personeelsleden hierover geïnformeerd. We hebben nog niet alles gedigitaliseerd.

Worden medewerkers geïnformeerd hoe lang persoonsgegevens worden opgeslagen?
Dat gaat nu in Youforce gebeuren. In Youforce worden de bewaartermijnen geregeld. Bepaalde dingen mogen 2 jaar, 5 jaar en 7 jaar bewaard worden. Zo kan je bijvoorbeeld een kopie paspoort 5 jaar bewaren.

Welke bewaartermijnen worden gehanteerd op de afdeling HRM PSA?
We hanteren de wettelijke bewaartermijn. Dat verschilt om wat voor soort persoonsgegevens het gaat en waar deze voor zijn opgeslagen. Een kopie paspoort bijvoorbeeld bewaren we 5 jaar na in dienst treding.

Hoe is de toegang tot personeelsbestanden geregeld?
De medewerkers van de afdeling HRM hebben alleen toegang tot die persoonsgegevens die nodig zijn voor de uitvoering van hun taken. Ik zelf bijvoorbeeld heb alleen toegang tot de persoonsgegevens van personeelsleden van de scholen die ik bedien.

Wordt de output van de gegevensverwerking doorgegeven aan andere afdelingen binnen de organisatie?
Om personele voorzieningen op te nemen in de financiën worden persoonsgegevens doorgegeven per email aan de afdeling F&A. In sommige gevallen zijn deze te herleiden naar de betreffende medewerkers.

Bijlage 5: Interview Security Officer

Is de organisatie zich bewust van de AVG?
Ja. Lucas onderwijs is halverwege 2017 begonnen met de implementatie van de AVG waarbij de lijn van het kennisnet is hierbij gevolgd. Fons Bos is eind 2017 toegevoegd als security officer aan de projectgroep AVG. Een security officer is niet verplicht. Een FG is wel verplicht. Een security officer heeft een uitvoerende taak en een FG heeft een controlerende rol. Lucas onderwijs is zich erg privacy bewust omdat Lucas onderwijs zich aan de wet moet houden en moet kunnen aantonen dat zij aan de AVG voldoet.

Is de organisatie bewust van de rollen verwerker en verwekingsverantwoordelijke?
Dat ligt weleens moeilijk. We hebben met veel organisaties werken die verwerkingsverantwoordelijken zijn zoals UWV en belastingdienst. Zij werken met onze gegevens maar zijn zelf verantwoordelijk. Op dit moment zijn er 170 verwerkingsovereenkomsten. Gezien de hoeveelheid overeenkomsten kan je wel stellen dat wij ons wel heel erg bewust zijn van de AVG. Er is weleens discussie wie nu verantwoordelijke is. In dat geval wordt een privacy-convenant opgesteld.
Er hoeft niet altijd een verwerkersovereenkomst te zijn omdat de organisaties gegevens voor hun zelf verwerken. Met deze organisaties worden privacyconvenanten opgesteld. Voor de belastingdienst of DUO hoeft dit bijvoorbeeld niet omdat zij gegevens verwerken vanuit een wettelijke taak. Grijs gebied zijn bijvoorbeeld de samenwerkingsverbanden waar de gemeente ook een rol in heeft.

Is een FG verplicht voor Lucas onderwijs?
Lucas Onderwijs is verplicht om een FG aan te stellen. Er is ook een FG aangesteld. Dit heeft te maken met de hoeveelheid en het soort gegevens is hierbij belangrijk. Lucas onderwijs verwerkt ook bijzondere persoonsgegevens. De heer Y. Bleeker is FG en heeft geen andere functie. De heer Bleeker is gepensioneerd en wordt voor een paar uur in de Week ingehuurd.
Lucas Onderwijs heeft bewust niet gekozen voor een externe FG. Lucas onderwijs had deze taak ook bij de accountant kunnen beleggen. Lucas heeft bewust gekozen om een eigen FG aan te stellen omdat je niet te veel last wil hebben van een FG. Hij heeft een controlerende functie en de wet is op meerdere manieren minder hard of zacht te interpreteren door een FG.

Wat zijn binnen Lucas onderwijs de taken van de FG?
De FG heeft een adviserende en controlerende taak. Een FG heeft een ontslagbescherming en heeft verregaande bevoegdheden en bij ernstige falen mag hij buiten het CvB handelen.

Is er een Security Officer werkzaam binnen Lucas onderwijs, zo ja, wat zijn de werkzaamheden?
Ik ben voor 0,5 FTE Security Officer de Lucas onderwijs. De definitie verschilt tussen een Privacy Officer en een Security Officer maar wordt weleens door elkaar gebruikt. Een Security Officer houdt zich met het hele domein van security, dus alles wat met security te maken heeft op het gebied van IT en een Privacy Officer alleen met privacy.

Waarom heeft Lucas onderwijs een Security officer aangesteld?
De AVG brengt heel veel uitvoering met zich mee en hebt je iemand nodig die kennis van de AVG omdat Lucas onderwijs een grote organisaties is. Er komen wekelijks vragen vanuit de organisaties met vragen over de AVG. De scholen moeten AVG bewust zijn maar hoeven niet alle ins en outs te kennen en hoeven geen AVG-specialist in dienst te hebben. Zo kunnen zij met al hun vragen bij mij terecht. De Security Officer signaleert en rapporteert naar de FG. Ik merk soms wel dat er een spanningsveld is omdat ik signaleer aan de FG. De FG heeft een ontslagbescherming maar ik als Security Officer heb dat niet. Medewerkers kunnen een melding van een datalek melden via het emailadres avg@lucasonderwijs.nl of telefonisch. Ik meld dit bij de directeur, bij de hoofd Informatiebeheer en bij de FG.

Wat zijn de taken van de Security Officer?

Ik ben verantwoordelijk voor de verwerkersovereenkomsten. Ik ben tevens het aanspreekpunt voor de organisatie m.b.t. AVG-vraagstukken. Daarnaast voer ik een eventuele Privacy Impact Assessment (PIA) uit. Ik geef advies op basis van de uitkomsten van een PIA om wel of niet te kiezen voor een softwarepakket. Zodra er discussie is om het wel of niet te doen informeer ik het CvB hierover en neemt het CvB een besluit hierover.

Wordt er een verwerkingsregister bijgehouden van de verwerking van persoonsgegevens? Zo ja, wie houdt deze bij?
Ik houd een dataregister bij van alle persoonsverwerkingen. Door het bijhouden van een dataregister krijgen we inzicht in wat er verwerkt wordt en wie de verwerker is. De dataverwerking wordt geclassificeerd. Dataverwerkingen met bijvoorbeeld bijzondere persoonsgegeven krijgen een hogere classificatie.

Zijn alle verwerkingsovereenkomsten met derden herzien bij de invoering van de AVG?
Nee, de bestaande verwerkingsovereenkomsten zijn niet bekeken. Deze zijn gelaten zoals ze waren. Wij zijn bezig om bestaande bewerkersovereenkomsten die voor de invoering van de AVG zijn afgesloten te vernieuwen.

Zijn alle verwerkingsovereenkomsten nu toereikend en voldoen deze aan de vereisten in de AVG?
De verwerkersovereenkomsten die mogelijk die niet aansluiten hebben wij wel bekeken wel. Wij zijn begonnen met 20 verwerkersovereenkomsten en momenteel zijn het er 170 geworden. Ik houd een register bij van alle verwerkersovereenkomsten.

Welke wijzigingen zijn er aangebracht in het gegevensverwerkingsproces toen de AVG werd ingevoerd?
Sinds de invoering van de AVG mogen geen we BSN-nummers gebruikt. Daarvoor worden nu voor personeelsleden met personeelsnummers gewerkt. Er zouden wel wijzigingen van technische maatregelen doorgevoerd moeten worden voor medewerkers die toegang hebben tot systemen waar personeelsgegevens worden verwerkt. Bijvoorbeeld doormiddel van de twee factor authenticatie (minder veilig als de Multi) of Multifactorautenticatie. Pakketten waar bijzondere personeelsgegevens worden verwerkt zou dit best weleens verplicht kunnen zijn.
Dat medewerkers bewust zijn van de AVG is wel te merken. Medewerkers komen met vragen als zij twijfels hebben wanneer gevraagd wordt om persoonsgegevens. Voorbeeld is een zwembad die om leerling gegevens vraagt of Gemeente Delft die om vraagt verzuimgegevens.

Hoe heeft Lucas Onderwijs haar activiteiten georganiseerd met betrekking tot beginselen van de AVG?
In het dataregister staan de grondslagen van de verwerking. Één grondslag is voldoende om persoonsgegevens te mogen verwerken. Als personeelslid wordt je weinig geïnformeerd over de verwerking van je personeelsgegevens. Een softwarepakket wordt pas aangeschaft nadat de MR hiermee heeft ingestemd.

Worden personeelsleden geïnformeerd over hun rechten?
Geen idee. Goeie vraag.

Wordt betrokkene geïnformeerd over de eventuele verwerking van haar of zijn persoonsgegevens en voor welk doel?
Nee, althans misschien wel. Ik ken de procedure niet wat er mee gebeurd.

Hoe past Lucas onderwijs het beginsel van minimale gegevensverwerking toe?
Bij dataminimalisatie kijken wij kritisch naar onze data en vragen ons of het noodzakelijk is voor de verwerking. Het is bijvoorbeeld niet relevant wat je afkomst is voor de salarisverwerking.

Medewerkers hebben zelf toegang tot hun persoonsgegevens. Zij kunnen eventuele wijzigingen zelf doorvoeren. Wij maken dagelijks een back up van data zodat deze niet verloren gaan. Maandelijks back-ups worden tot een jaar terug bewaard.

Wat is het beleid op de bewaartermijn voor de opslag van persoonsgegevens?
Lucas Onderwijs hanteert de wettelijke bewaartermijn voor zover dat van toepassing is.
Het documentsysteem M-files zit geen optie voor bewaartermijn classificatie. Dit zou wel moeten gebeuren zodat documenten waarin persoonsgegevens zijn opgenomen geclassificeerd kunnen worden en waar de bewaartermijn op toegepast kan worden. Bijvoorbeeld 7 jaar na uit dienst treding. Bij wettelijke grondslagen geld het wettelijke bewaartermijn. Als organisatie ben je verplicht om je hieraan te houden. Leerlinggegevens moeten 5 jaar nadat leerlingen de school hebben verlaten verwijderd worden. Leerlingdossier moeten na 2 jaar vernietigd. Dit gaat om alle gegevens van de leerlingen behalve die gegevens die nodig zijn voor de bekostiging. Dit gebeurt niet omdat de gegevens gebruikt worden voor de analyse van de schoolprestaties.

Welke maatregelen heeft Lucas onderwijs genomen om persoonsgegevens te beveiligen tegen ongeoorloofd toegang of onrechtmatige verwerking?
Voor Capisci is het niet nodig om een verwerkingsovereenkomst af te sluiten omdat deze op de eigen server draait. Lucas onderwijs is hierbij tevens verwerker. Lucas Onderwijs hanteert een cleandesk policy. Dat betekent dat je geen documenten op je bureau mag laten liggen.
Daarnaast hebben medewerkers alleen toegang in systemen tot die persoonsgegevens die noodzakelijk zijn voor de uitvoering van hun taken. Er is een functiescheiding autorisatie.
Binnen de organisatie zijn er systemen die zodanig zijn ontworpen dat wij intern de rechten bepalen (Privacy bij default). Je ziet echter dat softwareleveranciers steeds meer systemen ontwikkelen waarbij de rol van gebruiker reeds is bepaald (privacy by design.

Wordt medewerkers gevraagd om toestemming voor de verwerking van hun gegevens? en hoe wordt dit gedaan?
Niet bekend.

Informeert Lucas Onderwijs haar medewerkers over hun privacyrechten ten aanzien van de verwerking van hun persoonsgegevens? Zo ja, hoe worden zij geïnformeerd?
Niet bekend

Is een DPIA verplicht voor Lucas Onderwijs?
Een DPIA Is verplicht bij een nieuwe vorm van gegevensverwerking. Donderdag heb ik nog een DPIA gedaan.

Voert Lucas Onderwijs een DPIA uit? En zo ja wie voert dit uit?
Ja, ik voer de DPIA uit. Wij gebruiken hiervoor het model van de leverancier Norea, ik zal je het model doorsturen. De DPIA wordt bewaard voor het geval het AP hierop terugkomt. Uit een DPIA komen interessante vragen uit voort. Zo komt de vraag wat gebeurt er met de data wanneer het project is afgerond.

Welke maatregelen zijn er genomen om datalekken te voorkomen?
Ernstig datalek wordt meteen onderzocht. In overleg wordt worden maatregelen genomen om de datalek te verhelpen en wordt bekeken welke maatregelen genomen moeten om dit te voorkomen. Er wordt overlegd of de betrokkenen wel of niet te informeren. De medewerkers in de organisatie hoeven niet na te denken over de oplossing.

Wordt er overleg gepleegd met de AP indien risico's niet gedekt kunnen worden?

Op het gebied van persoonsgegevens is geen coulance. Indien uitkomsten van een PIA risico's aangeeft wordt altijd. Er zijn altijd risico's. Zijn de risico's aanvaardbaar. Zijn ze aanvaardbaar? Om hoeveel personeelsgegevens gaat het? Is het een pilot? Al deze vragen worden gesteld om vooraf een keuze te maken. Een DPIA moet je bewust maken wat je aan het doen bent.

Welke maatregelen worden genomen op het moment dat een risico niet gedekt kan worden?
In overleg met de leverancier de risico's terugbrengen. Soms ben je wel overgeleverd aan een leverancier.

Heeft Lucas onderwijs een PIA uitgevoerd? Wat zijn de uitkomsten hiervan als het gaat om de verwerking van persoonsgegevens van personeelsleden?
Lucas onderwijs heeft bij de invoering geen PIA uitgevoerd. Dat gebeurt alleen bij een nieuwe manier gegevensverwerking.

Is de bewaartermijn ergens vastgelegd in de organisatie?
Is vastgelegd. Elke afdeling moet bepalen wat de bewaartermijn is voor bepaalde persoonsgegevens.

Is er ook een PDCA-check?
Deze taak ligt bij de FG. Er is onlangs een risicoanalyse uitgevoerd. Daar komen aandachtspunten. Bepaalde risico's moeten direct worden aangepakt. Andere risico's zijn op de lange baan. De pdca is een drie jaar cyclus.

Bijlage 6: Verwerkersovereenkomst

Model Verwerkersovereenkomst 3.0

Deze Model Verwerkersovereenkomst is een bijlage bij het *Convenant Digitale Onderwijsmiddelen en Privacy* (hierna: het Convenant).

De nieuwe Model Verwerkersovereenkomst 3.0 komt in de plaats van eerdere Model verwerkersovereenkomsten uit 2015 en 2016. De uitgangspunten van deze Model Verwerkersovereenkomst 3.0 sluiten aan bij de bepalingen in het Convenant, geven invulling aan verplichtingen op grond van de Europese Algemene Verordening Gegevensbescherming (hierna: AVG), en de uitgangspunten zoals onder andere in (inter)nationale beveiligingsnormen, jurisprudentie en richtsnoeren van de toezichthouder zijn aangegeven.

Reeds afgesloten Verwerkersovereenkomsten op basis van de modellen uit 2015 en 2016 blijven hun gelding houden totdat deze verwerkersovereenkomsten door partijen worden beëindigd. Het uitgangspunt is dat met ingang van 25 mei 2018, het moment waarop de AVG van toepassing wordt, Onderwijsinstellingen en Leveranciers bij het aangaan van een verwerkersovereenkomst of bij vernieuwing van een bestaande verwerkersovereenkomst, de Model Verwerkersovereenkomst 3.0. gebruiken.

In het Convenant is afgesproken dat Onderwijsinstellingen en Leveranciers het actuele model gebruiken bij het maken van afspraken. Van de actuele Model Verwerkersovereenkomst kan alleen gemotiveerd en schriftelijk worden afgeweken.

Deze Model Verwerkersovereenkomst 3.0 bevat twee bijlagen:
In de Privacybijsluiter (Bijlage 1) wordt met name een beschrijving gegeven van de dienstverlening, producteigenschappen en welke categorieën Persoonsgegevens worden verwerkt en voor welke doeleinden.
In de Beveiligingsbijlage (Bijlage 2) wordt omschreven welke technische en organisatorische beveiligingsmaatregelen er worden getroffen. De beveiliging dient een continu punt van aandacht en zorg te blijven

Informatie over het Convenant en de model Verwerkersovereenkomst is te vinden op de website www.privacyconvenant.nl. Meer informatie en antwoorden op vragen over privacy en de wettelijke rechten en verplichtingen voor Onderwijsinstellingen zijn te vinden op de websites van de sectorraden PO-Raad, VO-raad, MBO Raad (saMBO-ICT) en bij Kennisnet.

Maart 2018

Partijen:
Het bevoegd gezag van <naam + rechtsvorm onderwijsinstelling>, geregistreerd onder BRIN-nummer <brin> bij de Dienst Uitvoering Onderwijs van het Ministerie van Onderwijs, gevestigd en kantoorhoudende aan <adres>, te (<postcode>) <plaats>, te dezen rechtsgeldig vertegenwoordigd door <functie + naam>, hierna te noemen: "**Onderwijsinstelling**".
en
De besloten vennootschap <Naam> B.V., gevestigd en kantoorhoudende aan <adres>, te (<postcode>) <plaats>, te dezen rechtsgeldig vertegenwoordigd door <functie + naam>, hierna te noemen: "**Verwerker**"

hierna gezamenlijk te noemen: "**Partijen**", of afzonderlijk: "**Partij**"

Overwegen het volgende:

Onderwijsinstelling en Verwerker zijn een overeenkomst aangegaan waarbij <**concrete omschrijving van de door Verwerker in opdracht van Onderwijsinstelling te leveren producten/diensten**>, ('de Product- en Dienstenovereenkomst'). Deze Product- en Dienstenovereenkomst leidt ertoe dat Verwerker in opdracht van Onderwijsinstelling Persoonsgegevens verwerkt.
Partijen wensen, mede gelet op het bepaalde in artikel 28 lid 3 Algemene Verordening Gegevensbescherming, in deze Verwerkersovereenkomst hun wederzijdse rechten en verplichtingen voor de Verwerking van Persoonsgegevens vast te leggen.

Komen het volgende overeen:

Artikel 1: Definities
In deze Verwerkersovereenkomst wordt verstaan onder:
Betrokkene, Verwerker, Derde, Persoonsgegevens, Verwerking van Persoonsgegevens en Verwerkingsverantwoordelijke: de begrippen zoals gedefinieerd in de AVG;
Bijlage(n): bijlage(n) bij het Convenant of de Verwerkersovereenkomst;
Convenant: het Convenant Digitale Onderwijsmiddelen en Privacy 3.0;
Convenantpartij: een tot het Convenant toegetreden Onderwijsinstelling of Leverancier;
Datalek: een inbreuk in verband met persoonsgegevens, zoals bedoeld in artikel 4 sub 12 AVG;
Digitaal Onderwijsmiddel: Leermiddelen en Toetsen, en School- en Leerlinginformatiemiddelen;
Initiatiefnemers: partijen die de initiatiefnemers zijn van het Convenant als opgenomen in de aanhef van het Convenant;
Instructies: geschreven of elektronisch gestuurde aanwijzing van de Verwerkingsverantwoordelijke aan de Verwerker in het kader van haar bevoegdheden zoals geformuleerd in deze Verwerkersovereenkomst of in de Product- en Dienstenovereenkomst.

Instructies worden verstrekt door en aan de contactpersonen van partijen zoals die zijn opgenomen in de Bijlage(n);
Keten iD: een pseudoniem van een persoonsgebonden nummer van een Onderwijsdeelnemer dat de Onderwijsdeelnemer niet langer direct identificeerbaar maakt. Hierna wordt dat pseudoniem opnieuw versleuteld tot het Keten iD, dat voor identificatiedoeleinden gebruikt wordt voor de toegang tot en het gebruik van Digitale Onderwijsmiddelen. Het Keten iD wordt ook ECK iD genoemd;
Leermiddelen en Toetsen: digitaal product en/of digitale dienst bestaande uit leerstof en/of toetsen en de daarmee samenhangende digitale diensten, gericht op onderwijsleersituaties, ten behoeve van het geven van onderwijs door of namens Onderwijsinstellingen;
Leverancier: leverancier van een Digitaal Onderwijsmiddel, zoals een distributeur, uitgever of leverancier van een administratiesysteem;
Model Verwerkersovereenkomst: het model voor een verwerkersovereenkomst die als bijlage is bijgevoegd bij het Convenant;
Onderwijsdeelnemer: onderwijsdeelnemer in het primair onderwijs, voortgezet onderwijs of middelbaar beroepsonderwijs;
Platform: het platform als bedoeld in artikel 8 van het Convenant, thans bekend als Edu-K;
Product- en Dienstenovereenkomst: de overeenkomst tussen Onderwijsinstelling en Verwerker, zoals omschreven in overweging a met inbegrip van een op basis van die overeenkomst gesloten overeenkomst tussen een Onderwijsdeelnemer en Leverancier voor het betreffende product of dienst;
Privacybijsluiter: één of meerdere privacybijsluiter(s) zoals opgenomen in de Bijlage(n) die van toepassing zijn op de aangeboden Digitale Onderwijsmiddelen;
Reglement: het reglement als bedoeld in artikel 8 lid 4 van het Convenant;
School- en Leerlinginformatiemiddelen: een digitaal product en/of digitale dienst ten behoeve van het onderwijs(proces), zoals een leerling-administratiesysteem, kernregistratiesysteem, studentinformatiesysteem, deelnemersadministratie, roostersysteem, ouderportaal, leerling- en oudercommunicatiesysteem, dashboards en kwaliteitsmanagementsystemen voor zover zij Persoonsgegevens van Onderwijsdeelnemers bevatten, een elektronische leeromgeving en een leerling volgsysteem;
Standaardattributenset: de door het Platform vastgestelde aanvullende gestandaardiseerde Persoonsgegevens van Onderwijsdeelnemers die naast het Keten iD gebruikt kunnen worden voor de toegang tot en het gebruik van Digitale Onderwijsmiddelen (zoals gepubliceerd op de website van het Platform);
Subverwerker: de partij die door Verwerker wordt ingeschakeld als Verwerker ten behoeve van de Verwerking van de Persoonsgegevens in het kader van de Model Verwerkersovereenkomst en de Product- en Dienstenovereenkomst;
AVG: de Algemene Verordening Gegevensbescherming (Verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG);

Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens: de toepasselijke (Unierechtelijke en lidstaatrechtelijke) wet- en regelgeving en/of (nadere) verdragen, verordeningen, richtlijnen, besluiten, beleidsregels, instructies en/of aanbevelingen van een bevoegde overheidsinstantie betreffende de Verwerking van Persoonsgegevens, tevens omvattende toekomstige wijziging hiervan en/of aanvulling hierop, inclusief lidstaatrechtelijke uitvoeringswetten van de AVG en de Telecommunicatiewet.

Artikel 2: Onderwerp en opdracht Verwerkersovereenkomst

Deze Verwerkersovereenkomst is van toepassing op de Verwerking van Persoonsgegevens in het kader van de uitvoering van de Product- en Dienstenovereenkomst.
De Onderwijsinstelling geeft Verwerker conform artikel 28 AVG opdracht en Instructies om Persoonsgegevens te verwerken namens de Onderwijsinstelling. De Instructies van de Onderwijsinstelling kunnen onder meer nader omschreven zijn in deze Verwerkersovereenkomst en de Product- en Dienstenovereenkomst.
De bepalingen uit de Verwerkersovereenkomst gelden voor alle Verwerkingen zoals opgenomen in Bijlage 1, die plaatsvinden ter uitvoering van de Product- en Dienstenovereenkomst. Verwerker brengt Onderwijsinstelling onverwijld op de hoogte indien Verwerker reden heeft om aan te nemen dat Verwerker niet langer aan de Verwerkersovereenkomst kan voldoen.

Artikel 3: Rolverdeling

Onderwijsinstelling is ten aanzien van de in diens opdracht uit te voeren Verwerkingen van Persoonsgegevens de Verwerkingsverantwoordelijke. Verwerker is Verwerker in de zin van de AVG. De Onderwijsinstelling heeft en houdt zelfstandige zeggenschap over het (het bepalen van) doel en de middelen van de Verwerking van de Persoonsgegevens.
Verwerker draagt er zorg voor dat de Onderwijsinstelling voorafgaande aan het sluiten van deze Verwerkersovereenkomst toereikend wordt geïnformeerd over de dienst(en) die de Verwerker verleent, en de uit te voeren Verwerkingen. De gegeven informatie stelt de Onderwijsinstelling in staat om te doorgronden welke Verwerkingen onlosmakelijk zijn verbonden met een aangeboden dienst en voor welke Verwerkingen Onderwijsinstelling een keuze kan maken voor eventueel aangeboden optionele diensten.
Onverminderd hetgeen elders in deze Verwerkersovereenkomst is bepaald, informeert Verwerker voorafgaand aan het sluiten van deze Verwerkersovereenkomst de Onderwijsinstelling in Bijlage 1 over de in lid 2 bedoelde diensten, waaronder eventuele optionele diensten, en de Verwerkingen die in dat kader plaatsvinden. De in Bijlage 1 opgenomen informatie moet in begrijpelijke taal zijn beschreven, waardoor Onderwijsinstelling geïnformeerd akkoord kan gaan met de afname van deze dienst(en) en de uitvoering van de bijbehorende Verwerkingen.
De Onderwijsinstelling neemt de in lid 2 van dit artikel genoemde Verwerking van de Persoonsgegevens op in een register van de verwerkingsactiviteiten[1] die onder hun verantwoordelijkheid plaatsvinden.

[1] Zie voor een voorbeeld de Aanpak IBP bij https://kn.nu/IBPonderwijs

Voor zover artikel 30 lid 5 AVG daartoe verplicht, houdt Verwerker conform artikel 30, lid 2 AVG een register bij van alle categorieën van verwerkingsactiviteiten die Verwerker ten behoeve van een Onderwijsinstelling verricht.
Onderwijsinstelling en Verwerker verstrekken elkaar over en weer alle benodigde informatie teneinde een goede naleving van de Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens mogelijk te maken.

Artikel 4: Privacyconvenant
Partijen onderschrijven de bepalingen in het Convenant.

Artikel 5: Gebruik Persoonsgegevens
Verwerker verplicht zich om de van Onderwijsinstelling verkregen Persoonsgegevens niet voor andere doeleinden of op andere wijze te gebruiken dan voor het doel, en conform de wijze waarvoor, de gegevens zijn verstrekt of aan hem bekend zijn geworden. Het is Verwerker derhalve niet toegestaan andere gegevensverwerkingen uit te voeren dan door de Onderwijsinstelling (schriftelijk dan wel elektronisch) aan Verwerker in het kader van de uitvoering van de Product- en Dienstenovereenkomst zijn opgedragen, behoudens een eventuele afwijkende Unierechtelijke of lidstaatrechtelijke bepaling, dan wel een rechterlijke uitspraak, voor zover daartegen geen beroep meer openstaat. In dat geval stelt Verwerker de Onderwijsinstelling voorafgaand aan de Verwerking van dat wettelijke voorschrift dan wel de rechterlijke uitspraak in kennis, tenzij dergelijke kennisgeving om gewichtige redenen van algemeen belang verboden is.
Een overzicht van onder meer de categorieën Persoonsgegevens en het doel waarvoor de Persoonsgegevens worden verwerkt, is uiteengezet in de Privacybijsluiter bij deze Verwerkersovereenkomst.
De Verwerker dient in de Privacybijsluiter aan te geven of de Privacybijsluiter ziet op een Leermiddel en Toets en/of een School- en Leerlinginformatiemiddel. Verwerker specificeert in de Privacybijsluiter voor welke, door de Verwerkersverantwoordelijke vastgestelde, doeleinden persoonsgegevens worden verwerkt bij het gebruik zijn product en/of dienst, en welke categorieën Persoonsgegevens daarbij worden verwerkt
Indien Verwerker in strijd met de AVG het doel en de middelen van de Verwerking van Persoonsgegevens bepaalt, wordt Verwerker met betrekking tot die Verwerking als Verwerkingsverantwoordelijke beschouwd.
SPECIFIEKE BEPALING IN GEVAL VAN UITWISSELING VAN HET ONDERWIJSKUNDIG RAPPORT: In aanvulling op het bepaalde in lid 4, is het Verwerker uitsluitend toegestaan om Persoonsgegevens te verstrekken aan een door Onderwijsinstelling aangewezen en geselecteerde andere onderwijsinstelling, na een concreet verzoek tot verstrekking van die onderwijsinstelling en op voorwaarde dat deze andere onderwijsinstelling haar administratieve onderwijsidentiteit (bijv. BRIN of OiN) aan Verwerker kenbaar heeft gemaakt. Indien de andere onderwijsinstelling niet beschikt over een administratieve onderwijsidentiteit zal Verwerker Persoonsgegevens alleen aan die andere onderwijsinstelling verstrekken op uitdrukkelijke instructie van Onderwijsinstelling.

SPECIFIEKE BEPALING VOOR VERWERKERSOVEREENKOMSTEN TUSSEN ONDERWIJSINSTELLINGEN EN DISTRIBUTEURS:

Convenantspartijen die Leermiddelen en Toetsen ontwikkelen en aanbieden (hierna te noemen: ***Leermiddelenleverancier****), zullen jaarlijks ten behoeve van het opstellen van de leermiddelenlijsten voor het eerstvolgende schooljaar, (welke leermiddelenlijsten ten behoeve van de uitvoering van de Product- en Dienstenovereenkomst worden opgesteld) de Privacy Bijsluiter voor die Leermiddelen en Toetsen aanvullen en/of wijzigen door het opnemen van de categorieën Persoonsgegevens en het gebruik dat van deze Persoonsgegevens wordt gemaakt (met betrekking tot de Leermiddelen en Toetsen die op de desbetreffende leermiddelenlijsten worden opgenomen).*

Verwerker (de distributeur) wisselt in opdracht van de Onderwijsinstelling gegevens uit met deze Leermiddelenleveranciers.

De Onderwijsinstelling is verantwoordelijk voor het maken en vastleggen van afspraken met iedere Leermiddelenleverancier in een Verwerkersovereenkomst.

Onderwijsinstelling vrijwaart Verwerker (distributeur) voor eventuele aanspraken van derden ten gevolge van het niet (tijdig) maken van Verwerkersafspraken met Leermiddelenleverancier, en de Onderwijsinstelling vrijwaart de Leermiddelenleverancier voor eventuele aanspraken van derden ten gevolge van het niet (tijdig) maken van Verwerkersafspraken met Verwerker (distributeur).

De verantwoordelijkheid van Verwerker (distributeur) voor het beheer van de Persoonsgegevens houdt op, op het moment dat de Leermiddelenleverancier die gegevens heeft ontvangen van Verwerker (distributeur).

Artikel 6: Vertrouwelijkheid

Verwerker garandeert dat hij alle Persoonsgegevens strikt vertrouwelijk zal behandelen ten opzichte van derden, waaronder overheidsinstanties. Verwerker zorgt er voor dat een ieder die hij betrekt bij de Verwerking van Persoonsgegevens, waaronder zijn werknemers, vertegenwoordigers en/of Subverwerkers, deze gegevens als vertrouwelijk behandelt. Verwerker waarborgt dat met de tot het Verwerken van de Persoonsgegevens geautoriseerde personen een geheimhoudingsovereenkomst of –beding is gesloten, of dat deze door een wettelijke verplichting tot geheimhouding zijn gebonden.

De in lid 1 bedoelde geheimhoudingsplicht geldt niet in de hierna genoemde gevallen:

voor zover Onderwijsinstelling uitdrukkelijk toestemming heeft gegeven om de Persoonsgegevens aan een Derde te verstrekken;

indien het verstrekken van de Persoonsgegevens aan een Derde noodzakelijk is gezien de aard van de door Verwerker aan Onderwijsinstelling te verlenen diensten; of

indien Verwerker op grond van een Unierechtelijke of lidstaatrechtelijke bepaling dan wel een gerechtelijke uitspraak, voor zover daartegen geen beroep meer openstaat, tot verstrekking verplicht is.

Verwerker onthoudt zich van verstrekking of bekendmaking van Persoonsgegeven aan een Derde, tenzij deze verstrekking of bekendmaking plaatsvindt in opdracht van Onderwijsinstelling respectievelijk wanneer dit noodzakelijk is om te voldoen aan een gerechtelijke uitspraak, voor zover daartegen geen beroep meer openstaat, of een op de Verwerker rustende wettelijke

verplichting. Onder wettelijke verplichtingen zijn begrepen Unierechtelijke of lidstaatrechtelijke bepalingen op grond waarvan Verwerker tot verstrekken verplicht is. In geval van een wettelijke verplichting, verifieert Verwerker voorafgaand aan de verstrekking de wettelijke grondslag en de identiteit van de partij die zich daarop beroept. Daarnaast stelt Verwerker - tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt - Onderwijsinstelling onmiddellijk, zo mogelijk voorafgaand aan de verstrekking, in kennis van de voor Onderwijsinstelling relevante informatie inzake deze verstrekking.
Verwerker zorgt er voor dat de onder diens gezag werkende medewerkers uitsluitend toegang hebben tot Persoonsgegevens voor zover noodzakelijk voor de vervulling van hun werkzaamheden.

Artikel 7: Beveiliging en controle
Met inachtneming van het bepaalde in artikel 32 AVG zal Verwerker, gelijk de Onderwijsinstelling, zorg dragen voor passende technische en organisatorische maatregelen om Persoonsgegevens te beveiligen en beschermen tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.
Naast de maatregelen als genoemd in artikel 32 lid 1 AVG, worden onder meer de volgende maatregelen - waar passend - genomen:
een passend beleid voor de beveiliging van de Verwerking van de Persoonsgegevens;
maatregelen om te waarborgen dat enkel geautoriseerde medewerkers toegang hebben tot de Persoonsgegevens die in het kader van de Verwerkersovereenkomst worden verwerkt;
het regelen van procedures rondom het verlenen van toegang tot Persoonsgegevens (waaronder een registratie- en afmeldprocedure voor toewijzing van toegangsrechten), en het in logbestanden vastleggen van gebeurtenissen betreffende gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen (vergelijkbaar met de toepasselijke ISO-normering, en/of vergelijkbaar met het geldende Certificeringsschema informatiebeveiliging en privacy ROSA). De Onderwijsinstelling wordt in de gelegenheid gesteld om deze logbestanden periodiek te controleren.
Partijen zullen de door haar getroffen beveiligingsmaatregelen periodiek evalueren en aanscherpen, aanvullen of verbeteren voor zover de eisen of (technologische) ontwikkelingen daartoe aanleiding geven.
In Bijlage 2 worden de afspraken tussen Partijen vastgelegd over de passende technische en organisatorische beveiligingsmaatregelen, alsmede over de inhoud, vorm en de werkwijze van de verklaringen die Verwerker verstrekt over de afgesproken beveiligingsmaatregelen.
De Verwerker stelt in goed overleg de Onderwijsinstelling in staat om effectief te kunnen voldoen aan zijn wettelijke verplichting om toezicht te houden op de naleving door de Verwerker van de technische en organisatorische beveiligingsmaatregelen alsmede op de naleving van de in artikel 8 genoemde verplichtingen ten aanzien van Datalekken.
In aanvulling op de voorgaande leden heeft Onderwijsinstelling te allen tijde het recht om, in overleg met de Verwerker en met inachtneming van een redelijke termijn, de naleving van Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, de Product-

en Dienstenovereenkomst en deze Verwerkersovereenkomst, waaronder de door Verwerker genomen technische en organisatorische beveiligingsmaatregelen, te (doen) controleren middels een audit uitgevoerd door een onafhankelijke gecertificeerde externe deskundige:
Partijen kunnen in onderling overleg afspreken dat de audit wordt uitgevoerd door een door Verwerker, in overleg met Onderwijsinstelling, in te schakelen externe deskundige die een derden-verklaring (TPM) afgeeft.
De auditor verstrekt het auditrapport alleen aan Partijen.
Partijen maken onderling afspraken over de omgang met de uitkomsten van de audit.
Partijen kunnen in onderling overleg afspreken dat, aan de hand van een geldige (inter)nationaal erkende certificering of een gelijkwaardig controle- of bewijsmiddel, een reeds uitgevoerde audit en daaruit afgegeven derden-verklaring gebruikt kan worden. Onderwijsinstelling wordt in dat geval geïnformeerd over de uitkomsten van de audit.
Partijen komen overeen dat de kosten van deze audit voor rekening komen van de Onderwijsinstelling, tenzij uit de audit (grote) gebreken blijken, die aan Verwerker kunnen worden toegerekend. In dat geval treden partijen in overleg over de verdeling van de kosten van de audit.

Artikel 8: Datalekken
Partijen hebben een passend beleid voor de omgang met Datalekken.
Indien Onderwijsinstelling of Verwerker een Datalek vaststelt, dan zal deze de andere Partij daarover *zonder onredelijke vertraging* informeren zodra hij kennis heeft genomen van dat Datalek. Verwerker verstrekt ingeval van een Datalek alle relevante informatie aan Onderwijsinstelling met betrekking tot het Datalek, waaronder informatie over eventuele ontwikkelingen rond het Datalek, en de maatregelen die de Verwerker treft om aan zijn kant de gevolgen van het Datalek te beperken en herhaling te voorkomen.
Verwerker informeert Onderwijsinstelling *onverwijld* indien een vermoeden bestaat dat een Datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen zoals bedoeld in artikel 34,lid 1, AVG.
Verwerker stelt bij een Datalek de Onderwijsinstelling in staat om passende vervolgstappen te (laten) nemen ten aanzien van het Datalek. Verwerker dient hierbij aansluiting te zoeken bij de bestaande processen die Onderwijsinstelling daartoe heeft ingericht. Partijen nemen zo spoedig mogelijk alle redelijkerwijs benodigde maatregelen om (verdere) schending of inbreuken betreffende de Verwerking de Persoonsgegevens, en meer in het bijzonder (verdere) schending van de Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, te voorkomen of te beperken.
In geval van een Datalek, voldoet Onderwijsinstelling aan eventuele wettelijke meldingsplichten.
In geval een Datalek bij Verwerker meerdere Onderwijsinstellingen in gelijke mate treft, kan Verwerker, na overleg met een of meerdere Verwerkingsverantwoordelijken, namens de Onderwijsinstellingen een melding doen van het Datalek aan de Autoriteit Persoonsgegevens. Van het voornemen hiervan zal Verwerker Onderwijsinstelling onverwijld (en zo mogelijk voorafgaand aan de melding) in kennis stellen.

In geval van het Datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, zal de Onderwijsinstelling de Betrokkenen informeren over het Datalek.
Partijen zullen te goeder trouw in onderling overleg afspraken maken over de redelijke verdeling van de eventuele kosten die verbonden zijn aan het voldoen aan de meldingsplichten.
Partijen documenteren alle Datalekken in een (incidenten)register, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen.
Over incidenten met betrekking tot de beveiliging, anders dan een Datalek, die vallen buiten het bereik van artikel 1 sub e van deze Verwerkersovereenkomst, informeert de Verwerker de Onderwijsinstelling conform de afspraken zoals neergelegd in Bijlage 2.

Artikel 9 Bijstand
Verwerker verleent Onderwijsinstelling bijstand bij het doen nakomen van de op Onderwijsinstelling rustende verplichtingen op grond van de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, zoals met betrekking - maar niet beperkt - tot:
het - voor zover redelijkerwijs mogelijk - vervullen van de plicht van Onderwijsinstelling om aan verzoeken van de in hoofdstuk III van de AVG vastgelegde rechten van de betrokkene binnen de wettelijke termijnen te voldoen, zoals een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens;
het uitvoeren van controles en audits zoals bedoeld in artikel 7 van deze Verwerkersovereenkomst;
het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) en een eventuele daaruit voortkomende verplichte voorafgaande raadpleging van de Autoriteit Persoonsgegevens;
het voldoen aan verzoeken van de Autoriteit Persoonsgegevens of een andere overheidsinstantie;
het voorbereiden, beoordelen en melden van datalekken zoals bedoeld in artikel 8 van deze Verwerkersovereenkomst.
Een klacht of verzoek van een Betrokkene of een verzoek of onderzoek van de Autoriteit Persoonsgegevens met betrekking tot de Verwerking van de Persoonsgegevens, wordt door de Verwerker, voor zover wettelijk is toegestaan, onverwijld doorgestuurd naar Onderwijsinstelling, die verantwoordelijk is voor de afhandeling van het verzoek.
Partijen brengen elkaar voor in redelijkheid verleende bijstand geen kosten in rekening. In het geval dat één van de Partijen kosten in rekening wil brengen, brengt deze partij de andere partij hiervan vooraf op de hoogte.

Artikel 10: Doorgifte aan derde landen buiten de Europese Economische Ruimte
Verwerker is uitsluitend gerechtigd tot doorgifte van Persoonsgegevens aan een derde land of internationale organisatie indien Onderwijsinstelling daarvoor specifieke Schriftelijke toestemming heeft gegeven, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling Verwerker tot Verwerking verplicht. In dat geval stelt Verwerker

Onderwijsinstelling voorafgaand aan de Verwerking Schriftelijk op de hoogte van deze bepaling, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt. Indien na toestemming van Onderwijsinstelling Persoonsgegevens worden doorgegeven aan derde landen buiten de Europese Economische Ruimte of aan een internationale organisatie zoals bedoeld in artikel 4 lid 26 AVG, dan zien Partijen er op toe dat dit alleen plaatsvindt conform wettelijke voorschriften en eventuele verplichtingen die in dit verband op Onderwijsinstelling rusten. Indien gegevens worden doorgegeven aan een derde land of een internationale organisatie, dan wordt dit in Bijlage 1 bij deze Verwerkers-overeenkomst aangegeven, inclusief een opgave van de landen waar, of internationale organisaties door wie, de Persoonsgegevens worden verwerkt. Daarbij wordt tevens aangegeven op welke wijze is voldaan aan de voorwaarden op basis van de AVG voor doorgifte van Persoonsgegevens aan derde landen of internationale organisaties.

Artikel 11: Inschakeling Subverwerker

Onderwijsinstelling geeft Verwerker door ondertekening van deze Verwerkers-overeenkomst toestemming tot het inschakelen van Subverwerkers, van wie de identiteit en vestigingsgegevens zijn opgenomen in de Privacybijsluiter.
Tijdens de duur van de Verwerkersovereenkomst licht Verwerker Onderwijsinstelling in over een voorgenomen toevoeging van een nieuwe Subverwerker of wijziging in de samenstelling van de bestaande Subverwerkers, waarbij Onderwijsinstelling de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken.
Verwerker is verplicht iedere Subverwerker via een overeenkomst of andere rechtshandeling minimaal dezelfde verplichtingen inzake gegevensbescherming op te leggen als in deze Verwerkersovereenkomst aan Verwerker zijn opgelegd. Hieronder vallen onder meer de verplichting om de Persoonsgegevens niet verder te Verwerken anders dan in het kader van deze Verwerkersovereenkomst is overeengekomen, en de verplichting tot het nakomen van de geheimhoudingsverplichtingen, meldingsverplichtingen, medewerkingsverplichtingen en beveiligingsmaatregelen met betrekking tot de Verwerking van Persoonsgegevens zoals in deze Verwerkersovereenkomst vastgelegd. Verwerker zal op verzoek van Onderwijsinstelling afschriften verstrekken van deze Verwerkers-overeenkomsten, of van de relevante passages uit de Verwerkersovereenkomst of een andere overeenkomst of een andere bindende rechtshandeling tussen Verwerker en de door deze overeenkomstig artikel 11, lid 1, van deze overeenkomst ingeschakelde Subverwerker.

Artikel 12: Bewaartermijnen en vernietiging Persoonsgegevens

Onderwijsinstelling zal Verwerker adequaat informeren over (wettelijke) bewaartermijnen die van toepassing zijn op de Verwerking van Persoonsgegevens door Verwerker. Verwerker zal de Persoonsgegevens niet langer Verwerken dan overeenkomstig deze bewaartermijnen.
Onderwijsinstelling verplicht Verwerker om de in opdracht van Onderwijsinstelling Verwerkte Persoonsgegevens bij de beëindiging van de Verwerkersovereenkomst te (doen) vernietigen, tenzij de Persoonsgegevens langer bewaard moeten worden, zoals in het kader van (wettelijke)

verplichtingen, dan wel op verzoek van de Onderwijsinstelling. De Onderwijsinstelling kan op eigen kosten een controle laten uitvoeren of vernietiging heeft plaatsgevonden.
Verwerker zal Onderwijsinstelling (schriftelijk of elektronisch) bevestigen dat vernietiging van de Verwerkte persoonsgegevens heeft plaatsgevonden.
Verwerker zal alle Subverwerkers die betrokken zijn bij de Verwerking van de Persoonsgegevens op de hoogte stellen van een beëindiging van de Verwerkers-overeenkomst en zal waarborgen dat alle Subverwerkers de Persoonsgegevens (laten) vernietigen.

Artikel 13: Aansprakelijkheid
Een Partij kan geen beroep doen op een aansprakelijkheidsbeperking, die is opgenomen in de Product- of Dienstenovereenkomst of andere tussen Partijen bestaande overeenkomst of regeling, ten aanzien van een door de andere Partij ingestelde:
verhaalsactie op grond van artikel 82 AVG; of
schadevergoedingsactie uit hoofde van deze Verwerkersovereenkomst, indien en voor zover de actie bestaat uit verhaal van een aan de Toezichthouder betaalde geldboete die geheel of gedeeltelijk toerekenbaar is aan de andere Partij.
Het bepaalde in dit artikel laat onverlet de rechtsmiddelen die de aangesproken partij op grond van de geldende wet- of regelgeving ter beschikking staat.
Het bepaalde in lid 1 sub b geldt onverminderd het bepaalde in artikel 14 lid 2.
Iedere Partij is verplicht de andere Partij zonder onnodige vertraging op de hoogte te stellen van een (mogelijke) aansprakelijkstelling of het (mogelijk) opleggen van een boete door de Toezichthouder, beiden in verband met deze Verwerkersovereenkomst. Iedere Partij is in redelijkheid verplicht de andere Partij informatie te verstrekken en/of ondersteuning te verlenen ten behoeve van het voeren van verweer tegen een (mogelijke) aansprakelijkstelling of boete, zoals bedoeld in de vorige volzin. De Partij die informatie verstrekt en/of ondersteuning verleent, is gerechtigd om eventuele redelijke kosten dienaangaande in rekening te brengen bij de andere Partij, Partijen informeren elkaar zo veel mogelijk vooraf over deze kosten.

Artikel 14: Tegenstrijdigheid en wijziging Verwerkersovereenkomst
In het geval van tegenstrijdigheid tussen de bepalingen uit deze Verwerkersovereenkomst en de bepalingen van de Product- en Dienstenovereenkomst, dan zullen de bepalingen van deze Verwerkersovereenkomst leidend zijn.
Indien Partijen van de artikelen in de Model Verwerkersovereenkomst door omstandigheden moeten afwijken, of deze willen aanvullen, dan zullen deze wijzigingen en/of aanvullingen door Partijen worden beschreven en gemotiveerd in een overzicht dat als Bijlage 3 aan deze Verwerkersovereenkomst zal worden gehecht. Het bepaalde in dit lid geldt niet voor aanvullingen en/of wijzigingen van de Bijlagen 1 en 2.
Bij belangrijke wijzigingen in het product en/of de (aanvullende) diensten die van invloed zijn op de Verwerking van de Persoonsgegevens wordt, alvorens de Onderwijsinstelling de keuze hiertoe aanvaardt, de Onderwijsinstelling in begrijpelijke taal geïnformeerd over de consequenties van deze wijzigingen. Onder belangrijke wijzigingen wordt in ieder geval verstaan: de toevoeging of

wijziging van een functionaliteit die leidt tot een uitbreiding ten aanzien van de te Verwerken Persoonsgegevens en de doeleinden waaronder de Persoonsgegevens worden Verwerkt. De wijzigingen zullen in Bijlage 1 worden opgenomen.
Wijzigingen in de artikelen van de Verwerkersovereenkomst kunnen uitsluitend in gezamenlijkheid worden overeengekomen.
In het geval enige bepaling van deze Verwerkersovereenkomst nietig, vernietigbaar of anderszins niet afdwingbaar is of wordt, blijven de overige bepalingen van deze Verwerkersovereenkomst volledig van kracht. Partijen zullen in dat geval met elkaar in overleg treden om de nietige, vernietigbare of anderszins niet afdwingbare bepaling te vervangen door een uitvoerbare alternatieve bepaling. Daarbij zullen partijen zoveel mogelijk rekening houden met het doel en de strekking van de nietige, vernietigde of anderszins niet afdwingbare bepaling.

Artikel 15: Duur en beëindiging
De looptijd van deze Verwerkersovereenkomst is gelijk aan de looptijd van de tussen Partijen gesloten Product- en Dienstenovereenkomst, inclusief eventuele verlengingen daarvan.
Deze Verwerkersovereenkomst eindigt van rechtswege bij de beëindiging van de Product- en Dienstenovereenkomst. De beëindiging van deze Verwerkersovereenkomst zal Partijen niet ontslaan van hun verplichtingen die voortvloeien uit deze Verwerkersovereenkomst die naar hun aard worden geacht ook na beëindiging voort te duren, waaronder in ieder geval artikel 5, lid 1, en de artikelen 6, 9 en 12.

Aldus overeengekomen, in tweevoud opgemaakt en ondertekend,

Onderwijsinstelling,	Verwerker,
Naam:	Naam:
Functie:	Functie:
Datum:	Datum:

Bijlage 1: Privacybijsluiter
Bijlage 2: Beveiligingsbijlage

BIJLAGE 1: PRIVACYBIJSLUITER [naam product/dienst]

[In de benaming van deze privacybijsluiter moet duidelijk worden gemaakt of het **distributie** of **gebruik** van digitale onderwijsmiddelen betreft]
Onderwijsinstellingen maken in toenemende mate gebruik van digitale toepassingen binnen het onderwijs. Bij het gebruik en levering van deze producten en diensten zijn gegevens nodig die te

herleiden zijn tot personen (zoals onderwijsdeelnemers). Onderwijsinstellingen moeten met Verwerkers afspraken maken over het gebruik van die Persoonsgegevens. Deze bijsluiter geeft onderwijsinstellingen informatie over de dienstverlening die Verwerker verleent en welke persoonsgegevens de Verwerker daarbij verwerkt. Alles bij elkaar eigenlijk over de vraag "wie, wat, waar, waarom en hoe" wordt omgegaan met de privacy van de betrokken personen van wie persoonsgegevens worden verwerkt.
Het gebruik van deze Privacybijsluiter helpt Onderwijsinstellingen om beter te begrijpen wat de werking van het product en/of dienst is en welke gegevens daarvoor worden uitgewisseld. De Privacybijsluiter is een bijlage bij de Modelverwerkersovereenkomst en omvat de Instructies voor de Verwerking van Persoonsgegevens van de Onderwijsinstelling aan de Verwerker.
In het kader van de herkenbaarheid is het wenselijk dat Verwerkers zo veel mogelijk op uniforme wijze gebruik maken van de Privacybijsluiter. Afwijkingen van dit model zijn weliswaar mogelijk, maar dienen bij voorkeur beperkt te blijven. Indien de ruimte in deze bijlage onvoldoende is om de benodigde informatie te beschrijven, is het mogelijk de informatie op te nemen in separate Bijlage(n), welke als volgt genummerd worden: "Bijlage 1A", "Bijlage 1B", etc.. Deze Bijlagen worden aan de Verwerkersovereenkomst gehecht.

Voor specifieke branches zoals uitgevers, distributeurs en leveranciers van student- en leerling-administratiesystemen, kunnen specifieke privacybijsluiters worden gemaakt die gebaseerd zijn op dit model. Deze specifieke modellen zijn afgestemd door de Initiatiefnemers van het Convenant. De modellen zijn te vinden op de website van het Platform: www.edu-k.nl/ibp.

A. Algemene informatie

Naam product en/of dienst :
Naam Verwerker en vestigingsgegevens :
Link naar leverancier en/of productpagina :
Beknopte uitleg en werking product en dienst :
Doelgroep (zoals po/vo, onderbouw/bovenbouw) :
Gebruikers onderwijsdeelnemers/ouders/verzorgers/ docenten/…

B. Omschrijving specifieke diensten

Omschrijving van de specifiek verleende diensten en bijbehorende Verwerkingen van Persoonsgegevens:
Verwerkingen die een onlosmakelijk onderdeel vormen van de aangeboden dienst.
[….]
[….]
[….]
Omschrijving van de optionele Verwerkingen die de Verwerker aanbiedt
[….]
[….]

MBO

Toelichting: Het gaat hier om aanvullende diensten en bijhorende Verwerkingen die geen onlosmakelijk onderdeel vormen van de aangeboden dienst. Dit zijn bijvoorbeeld optionele diensten voor de Onderwijsinstelling die behulpzaam kunnen zijn voor de Onderwijsinstelling t.b.v. het primaire (leer)proces en administratieve werkzaamheden.

De Onderwijsinstelling dient een keuze te maken en daarbij opdracht te geven om persoonsgegevens te verwerken, voor het afnemen van deze diensten. Dat kan door de keuze schriftelijk aan te geven in deze bijlage (bijvoorbeeld door het aanvinken van een tick-box☑).

De opdracht kan ook worden verleend doordat de Onderwijsinstelling in de praktijk de dienst activeert, bijvoorbeeld door een product of dienst aan of uit zetten. De Onderwijsinstelling die op deze wijze de keuze maakt, dient dit op basis van eerder verstrekte informatie (zoals bijvoorbeeld opgenomen in deze bijsluiter) te doen.

C. Doeleinden voor het verwerken van gegevens

De Verwerker dient in deze Bijsluiter expliciet aan te geven of deze:

I. leverancier is van een digitaal product en/of digitale dienst bestaande uit leerstof en/of toetsen, of

II. (tevens) leverancier is van een School- en Leerlinginformatiemiddel.

Ad I. Indien de Verwerker leverancier is van een digitaal product en/of digitale dienst bestaande uit Leermiddelen en Toetsen, dan zijn de volgende mogelijke doelstellingen van gegevensverwerking in het kader van deze producten en diensten van toepassing:

a. het met gebruikmaking van het Digitale Onderwijsmiddel geven en volgen van onderwijs en het begeleiden en volgen van Onderwijsdeelnemers, waaronder:

de opslag van leer- en toetsresultaten;

het terugontvangen door de Onderwijsinstelling van leer- en toetsresultaten;

de beoordeling van leer- en toetsresultaten om leerstof en toetsmateriaal te kunnen verkrijgen dat is afgestemd op de specifieke leerbehoefte van een Onderwijsdeelnemer;

analyse en interpretatie van leerresultaten;

het kunnen uitwisselen van leer- en toetsresultaten tussen Digitale Onderwijsmiddelen.

b. het geleverd krijgen/in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier;

c. het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie;

d. de beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de, met behulp van het Digitale Onderwijsmiddel Verwerkte Persoonsgegevens.

e. de continuïteit en goede werking van het Digitale Onderwijsmiddel conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen na geconstateerde fouten of onjuistheden en het krijgen van ondersteuning;

f. onderzoek en analyse op basis van strikte voorwaarden, vergelijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek, ten behoeve van het (optimaliseren van het) leerproces of het beleid van de Onderwijsinstelling;
g. het door de Onderwijsinstelling voor onderzoeks- en analyse doeleinden beschikbaar kunnen stellen van volledig geanonimiseerde Persoonsgegevens om daarmee de kwaliteit van het onderwijs te verbeteren.
h. het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen.
i. De uitvoering of toepassing van een andere wet

Ad II. (Alleen) indien de Verwerker (tevens) leverancier is van een digitaal product en/of digitale dienst bestaande uit een School- en Leerlinginformatiemiddel dan zijn de volgende mogelijke doelstellingen van gegevensverwerking in het kader van deze producten en diensten van toepassing:
a. de organisatie, het geven en volgen van onderwijs, het begeleiden en volgen van Onderwijsdeelnemers of het geven van school- en studieadviezen, waaronder:
de indeling en aanpassing van roosters;
de analyse en interpretatie van leerresultaten;
het bijhouden van persoonlijke (waaronder medische) omstandigheden van een Onderwijsdeelnemer en de gevolgen daarvan voor het volgen van onderwijs;
het begeleiden en ondersteunen van leerkrachten en andere medewerkers binnen de Onderwijsinstelling;
de communicatie met Onderwijsdeelnemers en ouders en medewerkers van de onderwijsinstelling;
financieel beheer;
monitoring en verantwoording, ten behoeve van met name: (prestatie)metingen van de Onderwijsinstelling, kwaliteitszorg, tevredenheidsonderzoek, effectiviteitsonderzoek van onderwijs(vorm) of de geboden ondersteuning van Onderwijsdeelnemers bij passend onderwijs;
het behandelen van geschillen.
het uitwisselen van Persoonsgegevens met Derden, waaronder:
toezichthoudende instanties en zorginstellingen in het kader van de uitvoering van hun (wettelijke) taak;
samenwerkingsverbanden in het kader van passend onderwijs, regionale overstappen;
partijen betrokken bij de invulling van stage of leer-/ werkplekken voor zover noodzakelijk en wettelijk toegestaan;
Onderwijsinstellingen ingeval van overstappen tussen onderwijsinstellingen en bij vervolgonderwijs.
b. het geleverd krijgen/in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier;
c. het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie;

d. de beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de, met behulp van het Digitale Onderwijsmiddel, Verwerkte Persoonsgegevens.
e. de continuïteit en goede werking van het Digitale Onderwijsmiddel conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen na geconstateerde fouten of onjuistheden en het krijgen van ondersteuning;
f. onderzoek en analyse op basis van strikte voorwaarden, vergelijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek, ten behoeve van het (optimaliseren van het) leerproces of het beleid van de Onderwijsinstelling;
g. het door de Onderwijsinstelling voor onderzoeks- en analyse doeleinden beschikbaar kunnen stellen van volledig geanonimiseerde Persoonsgegevens om daarmee de kwaliteit van het onderwijs te verbeteren.
h. het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen.
i. De uitvoering of toepassing van een andere wet

D. Categorieën en soorten persoonsgegevens

1. Omschrijving van de categorieën Betrokkenen over wie Persoonsgegevens worden verwerkt, en de categorieën persoonsgegevens van de Betrokkenen:

Van toepassing	Categorie	Toelichting
	1. Contactgegevens	naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens; Beperkte set = naam, e-mail, opleiding; Persoonlijke set = geboortedatum, geslacht;
	2. Onderwijs-deelnemer-nummer	een administratienummer dat onderwijsdeelnemers identificeert
	3.Nationaliteit en geboorteplaats	
	4**. Ouders, voogd**	gegevens als bedoeld onder 1, van de ouders/verzorgers van onderwijsdeelnemers
	5. Medische gegevens	gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de betrokkene of op eigen verzoek, een en ander voor zover noodzakelijk voor het onderwijs;
	6. Godsdienst	gegevens betreffende de godsdienst of levensovertuiging van de betrokkene, voor zover die noodzakelijk zijn voor het onderwijs, of op

		eigen verzoek, een en ander voor zover noodzakelijk voor het onderwijs;
	7. Studievoortgang	gegevens betreffende de aard en het verloop van het onderwijs, alsmede de behaalde studieresultaten; te weten: klas / leerjaar / ILT code Examinering Studievoortgang en/of Studietraject Begeleiding onderwijsdeelnemers, inclusief handelingplan Aanwezigheidsregistratie
	8. Onderwijsorganisatie	gegevens met het oog op de **organisatie van het onderwijs** en het verstrekken of ter beschikking stellen van leermiddelen;
	9. Financiën	gegevens met het oog op het berekenen, vastleggen en innen van inschrijvingsgelden, school- en lesgelden en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten, alsmede bankrekeningnummer van de betrokkene;
	10. Beeldmateriaal	foto's en videobeelden **(beeldmateriaal)** met of zonder geluid van activiteiten van de instelling of het instituut;
	11. Docent, zorg-coördinator, intern begeleider, decaan, mentor	gegevens van **docenten en begeleiders,** voor zover deze gegevens van belang zijn voor de organisatie van het instituut of de instelling en het geven van onderwijs, opleidingen en trainingen;
	12 Overige gegevens, te weten ….	andere dan de onder 1 tot en met 11 bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere wet. **Wel moet worden vermeld om welke gegevens het gaat.**
	13. BSN/PGN	
	14. Keten-ID (ECK-ID)	unieke iD voor de 'educatieve contentketen'. hiermee kunnen onderwijsinstellingen gegevens delen, zonder dat ze direct herleidbaar zijn naar onderwijsdeelnemers of docenten.

3. Door de Verwerker te hanteren specifieke bewaartermijnen van Persoonsgegevens (of toetsingscriteria om dit vast te stellen):
[….]

E. Opslag Verwerking Persoonsgegevens:
Plaats/Land van opslag en Verwerking van de Persoonsgegevens:

F. Subverwerkers
Onderwijsinstelling geeft Verwerker door ondertekening van de Verwerkersovereenkomst een algemene schriftelijke toestemming voor het inschakelen van een Subverwerker. Verwerker heeft het recht gebruik te gaan maken van andere Subverwerkers, mits daarvan voorafgaand mededeling wordt gedaan aan Onderwijsinstelling, en Onderwijsinstelling daartegen bezwaar kan maken binnen een redelijke periode.
Verwerker maakt ten tijde van het afsluiten van de Verwerkersovereenkomst gebruik van de volgende Subverwerkers:
[partijnaam en vestigingsplaats, beknopte omschrijving taak/dienst waaruit blijkt welke informatie wordt Verwerkt door deze Subverwerker, plaats/land van opslag en Verwerking Persoonsgegevens*]*
Opmerking: indien de Persoonsgegevens buiten de EER worden verwerkt wordt apart opgave gedaan van de landen waar de Persoonsgegevens worden verwerkt én op welke wijze is gewaarborgd dat de gegevens rechtmatig kunnen worden doorgegeven.

G. Contactgegevens
Voor vragen of opmerkingen over deze bijsluiter of de werking van dit product of deze dienst, kunt u terecht bij: [contactgegevens].

G. Versie
[versie nummer en datum laatste aanpassing]

Deze Privacybijsluiter maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 3.0, een initiatief van de PO-Raad, VO-raad, MBO Raad de verschillende betrokken ketenpartijen (GEU, KBb-E en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u hier: http://www.privacyconvenant.nl.

BIJLAGE 2: BEVEILIGINGSBIJLAGE

De Verwerker is overeenkomstig de AVG en artikel 7 en 8 Model Verwerkersovereenkomst verplicht passende technische en organisatorische maatregelen te nemen ter beveiliging van de Verwerking van Persoonsgegevens, en om die maatregelen aan te tonen. Deze bijlage geeft een beknopte beschrijving en opsomming van die maatregelen.

Normen informatiebeveiliging

Verwerker is verplicht om aan Onderwijsinstelling aan te tonen of en op welke wijze passende technische en organisatorische maatregelen zijn genomen om te waarborgen en te kunnen aantonen dat de verwerking plaatsvindt in overeenstemming met de AVG en de Model Verwerkersovereenkomst.

Voor het toepassen en aantonen van de technische maatregelen, kan Verwerker gebruik maken van (zo snel als redelijkerwijs mogelijk de meest recente versie van) het in het onderwijs ontwikkelde '*Certificeringsschema informatiebeveiliging en privacy ROSA*'[2]. Dat schema voorziet in een baseline van (beveiligings)maatregelen waarmee organisaties dit aantoonbaar kunnen maken.

Indien Verwerker voornoemd Certificeringsschema gebruikt, dan mag gebruik worden gemaakt van een standaard beveiligingsbijlage die is afgestemd door de Initiatiefnemers van het Convenant. Deze afgestemde bijlage 2 is te vinden op de website van het Platform en komt in de plaats van deze model bijlage 2: www.edu-k.nl/ibp.

Verwerker kan ook gebruik maken van andere certificeringsmechanismen en/of (inter)nationaal erkende normen en standaarden voor informatiebeveiliging, mits die een gelijkwaardig of hoger niveau van beveiliging bieden en de door Verwerker genomen maatregelen aan de Onderwijsinstelling inzichtelijk worden gemaakt.

Minimale beveiligingsmaatregelen en aantoonbaarheid

Verwerker plaatst op deze plek in de bijlage een verklaring waaruit blijkt dat voldaan wordt aan passende technische maatregelen voor de beveiliging van de Verwerking van Persoonsgegevens. Deze verklaring bevat ten minste:

Een classificatie van het product of de dienst op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid;

Een beschrijving in welke mate aan de hieronder genoemde minimale beveiligingsmaatregelen in het kader van artikel 32 AVG wordt voldaan;

Verwerker heeft een passend beleid voor de beveiliging van de Verwerking van de Persoonsgegevens, waarbij het beleid periodiek wordt geëvalueerd en – zo nodig – aangepast;

Verwerker heeft de Persoonsgegevens die worden Verwerkt geclassificeerd op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid en heeft op basis van die classificatie beveiligingsmaatregelen genomen om de risico's voor de Verwerking van Persoonsgegevens te beperken;

Verwerker neemt maatregelen zodat via een systeem van autorisatie enkel geautoriseerde medewerkers toegang kunnen verkrijgen tot de Verwerking van Persoonsgegevens in het kader

[2] https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/

van de Verwerkersovereenkomst. Hierbij heeft Verwerker procedures vastgesteld en gedeeld met de Onderwijsinstelling voor de identificatie, autorisatie en authenticatie van medewerkers alsmede rondom de registratie, aanmelding en afmelding van de medewerkers;
Verwerker zorgt dat de toegang tot het product of de dienst beveiligd is door middel van een passend beleid voor wachtwoorden dat aansluit bij de stand van de techniek;
Verwerker heeft procedures voor het verlenen van toegang tot Persoonsgegevens (waaronder een registratie- en afmeldprocedure voor toewijzing van toegangsrechten), en het in logbestanden vastleggen van gebeurtenissen betreffende gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen (vergelijkbaar met de toepasselijke ISO-normering en/of vergelijkbaar met het Certificeringsschema informatiebeveiliging en privacy ROSA). De Onderwijsinstelling wordt in de gelegenheid gesteld om deze logbestanden periodiek te controleren;
Verwerker heeft maatregelen genomen om de Persoonsgegevens te beschermen tegen verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.
Verwerker maakt bij de beveiliging van de Verwerking van Persoonsgegevens gebruik van een (inter)nationale beveiligingsnorm;
Verwerker heeft maatregelen genomen om zwakke plekken te identificeren ten aanzien van de Verwerking van Persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan de Onderwijsinstelling.
Een toetsing van getroffen maatregelen aan (inter)nationaal erkende normen en standaarden voor informatiebeveiliging.

Beveiligingsincidenten en/of datalekken:
In geval van een (vermoeden van) beveiligingsincident en/of datalek, kan Onderwijsinstelling contact opnemen met: [contactgegevens helpdesk/servicedesk voor beveiligingsincidenten]

De contactpersoon voor Verwerker is: [contactgegevens Onderwijsinstelling voor beveiligingsincidenten]

Informeren over Datalekken en/of incidenten met betrekking tot beveiliging
Er is een procedure over het informeren in geval van datalekken en/of incidenten met betrekking tot beveiliging, en bevat ten minste te volgende punten:
De wijze waarop monitoring en identificatie van incidenten plaatsvindt,
De wijze waarop informatie wordt gedeeld:
Op welke manier (via e-mail, telefoon);
Aan wie gericht (contactpersonen en contactgegevens);
Met wie kan (bij vervolgacties) contact worden opgenomen.
Informatie die in ieder geval over een incident gedeeld moet worden

De kenmerken van het incident, zoals: datum en tijdstip constatering, samenvatting incident, kenmerk en aard incident (op wat voor onderdeel van de beveiliging ziet het, hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van persoonsgegevens);
De oorzaak van het beveiligingsincident;
De maatregelen die getroffen zijn om eventuele/verdere schade te voorkomen;
Benoemen van betrokkenen die gevolgen kunnen ondervinden van het incident, en de mate waarin;
De omvang van de groep betrokkenen;
Het soort gegevens dat door het incident wordt getroffen (met name bijzondere gegevens, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).
Eventuele afspraken of, en zo ja hoe, Verwerker een melding aan de Autoriteit Persoonsgegevens kan verrichten.

Versie [versie nummer en datum laatste aanpassing]

Deze Beveiligingsbijlage maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 3.0, een initiatief van de PO-Raad, VO-raad, MBO Raad de verschillende betrokken ketenpartijen (GEU, KBb-E en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u hier: http://www.privacyconvenant.nl.

Bijlage 7: Privacyreglement

Privacyreglement Stichting Lucas Onderwijs

Privacyreglement voor Stichting Lucas Onderwijs

1. Toepasselijkheid	Dit reglement geldt voor de gehele organisatie die deel uitmaakt van Stichting Lucas Onderwijs (hierna te noemen: Lucas Onderwijs). Lucas Onderwijs is gevestigd aan de Saffierhorst 105 te Den Haag.
2. Definities	
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'), zoals bijvoorbeeld naam, adres, geboortedatum, titel(s), geslacht, adres, telefoonnummer, e-mailadres, functie, personeelsnummer, medische rapportages, inhoud van e-mails, prestaties/cijfers, brieven, klachten, foto's, video's, IP-adressen, tracking cookies, loginnamen en wachtwoorden.
Verwerking van persoonsgegevens	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, geautomatiseerd of handmatig, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.
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.
Betrokkene	Degene op wie een persoonsgegeven betrekking heeft, en die al dan niet wordt vertegenwoordigd door een wettelijk vertegenwoordiger. Betrokkenen kunnen bijvoorbeeld zijn: leerlingen, ouders, medewerkers en bezoekers.
Wettelijk vertegenwoordiger	Degene die het ouderlijk gezag over een minderjarige uitoefent. Meestal zal dit een ouder zijn, maar het kan ook gaan om een voogd. Als een leerling 16 jaar of ouder is, beslist hij in voorkomende gevallen zelf over zijn privacy.
Verwerkingsverantwoordelijke	De entiteit die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. In het kader van dit reglement is het bevoegd gezag, te weten de Stichting Lucas Onderwijs (bevoegd gezag, vertegenwoordigd door het College van Bestuur, de verwerkingsverantwoordelijke.
Verwerker	De natuurlijke persoon of rechtspersoon die ten behoeve van de verwerkingsverantwoordelijke (bevoegd gezag) persoonsgegevens verwerkt, zoals bijvoorbeeld de leverancier van een leerlingvolgsysteem of leerling-administratiesysteem. Een verwerker heeft een uitvoerende taak, ten behoeve van de activiteiten van de verwerkingsverantwoordelijke.
Derde	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, de verwerkingsverantwoordelijke, de verwerker, of de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om persoonsgegevens te verwerken.
Bevoegd gezag	Stichting Lucas Onderwijs, de verwerkingsverantwoordelijke in de zin van dit reglement.

3. Reikwijdte en doelstelling	1. Dit reglement stelt regels over de verwerking van persoonsgegevens van alle betrokkenen bij de organisatie, waaronder leerlingen en hun wettelijk vertegenwoordigers, medewerkers, bezoekers en externe relaties (bijv. leveranciers en opdrachtnemers). 2. Dit reglement is van toepassing op alle persoonsgegevens van de betrokkene die door het bevoegd gezag worden verwerkt. Het reglement heeft tot doel: a. de persoonlijke levenssfeer van de betrokkenen te beschermen tegen verkeerd en onbedoeld gebruik van de persoonsgegevens; b. vast te stellen met welk doel en op welke (juridische) grondslag persoonsgegevens binnen Het bevoegd gezag worden verwerkt; c. ook overigens te borgen dat persoonsgegevens binnen het bevoegd gezag rechtmatig, transparant en behoorlijk worden verwerkt; d. de rechten van betrokkenen vast te leggen en te borgen dat deze rechten Het bevoegd gezag worden gerespecteerd.
4. Doelen van de verwerking van persoonsgegevens	Bij de verwerking van persoonsgegevens houdt het bevoegd gezag zich aan de relevante wet- en regelgeving waaronder de Algemene Verordening Gegevensbescherming (AVG), de uitvoeringswet AVG en de onderwijswetgeving.
Doelen	1. De verwerking van persoonsgegevens vindt plaatst voor: a. de organisatie of het geven van het onderwijs, de begeleiding van leerlingen, het voorzien in hun (extra) ondersteuningsbehoefte, dan wel het geven van studieadviezen; b. het verstrekken en/of ter beschikking stellen van leermiddelen; c. het bewaken van de veiligheid binnen de scholen en het beschermen van eigendommen van medewerkers, leerlingen en bezoekers; d. het bekend maken van informatie over de organisatie en leermiddelen als bedoeld, onder a en b, alsmede van informatie over de leerlingen op de eigen website; e. het bekend maken van de activiteiten van de organisatie, bijvoorbeeld op de website van Het bevoegd gezag of van de scholen, in brochures of de schoolgids of via social media; f. het berekenen, vastleggen en innen van inschrijvingsgelden, school- en lesgelden en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten, waaronder begrepen het in handen van derden stellen van vorderingen; g. het aanvragen van bekostiging, het behandelen van geschillen daarover en het doen uitoefenen van accountantscontrole; h. het onderhouden van contacten met oud-leerlingen; i. het aangaan en uitvoeren van arbeidsovereenkomsten, samenwerkingsrelaties met opdrachtnemers en contracten met leveranciers; j. de uitvoering of toepassing van wet- en regelgeving; k. juridische procedures waarbij Het bevoegd gezag betrokken is. 2. De verwerking van persoonsgegevens mag ook plaatsvinden voor doelen die verenigbaar zijn met de doelen zoals beschreven in lid 1.
5. Doelbinding	Persoonsgegevens worden uitsluitend gebruikt voor zover dat gebruik verenigbaar is met de omschreven doelen van de verwerking. Het bevoegd gezag verwerkt niet meer gegevens dan noodzakelijk is om de betreffende doelen te bereiken.
6. Soorten persoonsgegevens	De categorieën van persoonsgegevens zoals deze binnen het bevoegd gezag worden verwerkt, worden geregistreerd in een verwerkingsregister.
7. Grondslag verwerking	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 Het bevoegd gezag is opgedragen.

b. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op Het bevoegd gezag 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 Het bevoegd gezag 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 toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden.

8. Bewaartermijnen

Het bevoegd gezag bewaart persoonsgegevens niet langer dan noodzakelijk is voor het doel waarvoor deze worden verwerkt, tenzij het langer bewaren van de persoonsgegevens op grond van wet- of regelgeving verplicht is.

9. Toegang

Binnen de organisatie van Lucas Onderwijs 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 de school opgenomen persoonsgegevens aan:
a. de verwerker die van het bevoegd gezag 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 het bevoegd gezag 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.

10. Beveiliging en geheimhouding

1. Het bevoegd gezag 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. 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.
3. Een ieder die betrokken is bij de verwerking van persoonsgegevens binnen Het bevoegd gezag 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.

11. Verstrekken gegevens aan derden	Het bevoegd gezag kan persoonsgegevens aan derden verstrekken als daarvoor een grondslag bestaat in de zin van artikel 7 van dit reglement.
12. Sociale media	Voor het gebruik van persoonsgegevens in sociale media, zijn aparte afspraken gemaakt in het sociale mediaprotocol van het bevoegd gezag.
13. Rechten betrokkenen	1. Het bevoegd gezag erkent de rechten van betrokkenen, handelt daarmee in overeenstemming en bewerkstelligt dat betrokkenen deze rechten daadwerkelijk kunnen uitoefenen. Het betreft in het bijzonder de volgende rechten:
Inzage	a. Een betrokkene heeft recht op inzage van de door het bevoegd gezag verwerkte persoonsgegevens die op hem betrekking hebben, behalve voor zover het gaat om werkdocumenten, interne notities en andere documenten die uitsluitend bedoeld zijn voor intern overleg en beraad. Indien en voor zover dit recht op inzage ook de rechten en vrijheden van anderen raakt, bijvoorbeeld als in de documenten ook persoonsgegevens van anderen dan de betrokkene zijn vermeld, kan het bevoegd gezag het recht op inzage beperken. Bij het verstrekken van de betreffende gegevens verschaft het bevoegd gezag voorts informatie over: - de verwerkingsdoeleinden; - de categorieën van persoonsgegevens die worden verwerkt; - de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt; - (indien van toepassing) ontvangers in derde landen of internationale organisaties; - (indien mogelijk) hoe lang de gegevens worden bewaard; - dat de betrokkene het recht heeft om te verzoeken dat de persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van de persoonsgegevens wordt beperkt, alsmede dat hij het recht heeft om bezwaar te maken tegen de verwerking van de persoonsgegevens; - het feit dat de betrokkene een klacht kan indienen bij de Autoriteit Persoonsgegevens; - de bron van de persoonsgegevens, indien de persoonsgegevens niet van de betrokkene zelf zijn verkregen; - het eventueel toepassen van geautomatiseerde besluitvorming en de betreffende onderliggende logica en het belang en de gevolgen voor de betrokkene; - de passende waarborgen indien de persoonsgegevens worden doorgegeven aan een derde land of een internationale organisatie.
Verbetering, aanvulling, verwijdering	b. Het bevoegd gezag verbetert de persoonsgegevens van een betrokkene in het geval de betrokkene terecht heeft aangegeven dat de gegevens onjuist zijn, en het bevoegd gezag vult de persoonsgegevens van een betrokkene aan indien de betrokkene terecht om aanvulling heeft verzocht. Voorts kan de betrokkene verzoeken om verwijdering van zijn persoonsgegevens. Het bevoegd gezag gaat daartoe over indien is voldaan aan een wettelijke grondslag voor het verzoek, tenzij het onmogelijk is om aan het verzoek te voldoen of dit een onredelijke inspanning zou vergen.
Bezwaar	c. Indien het bevoegd gezag persoonsgegevens verwerkt op de grondslag van artikel 7 onder a of artikel 7 onder d van dit reglement, kan de betrokkene bezwaar maken tegen de verwerking van zijn persoonsgegevens. In dat geval staakt het bevoegd gezag de verwerking van de betreffende persoonsgegevens, behalve als naar het oordeel van het bevoegd gezag het belang van het

bevoegd gezag, het belang van derden of het algemeen belang in het betreffende concrete geval zwaarder weegt.

Beperken verwerking

d. De betrokkene kan voorts verzoeken om de verwerking van zijn persoonsgegevens te beperken, namelijk indien hij een verzoek tot verbetering heeft gedaan, indien hij bezwaar heeft gemaakt tegen de verwerking, als de persoonsgegevens niet meer nodig zijn voor het doel van de verwerking of als de gegevensverwerking onrechtmatig is. Het bevoegd gezag staakt dan de verwerking, tenzij de betrokkene toestemming heeft gegeven voor de verwerking, Het bevoegd gezag de gegevens nodig heeft voor een rechtszaak of de verwerking nodig is ter bescherming van de rechten van een andere persoon of vanwege gewichtige redenen.

Kennisgevingsplicht

e. Als het bevoegd gezag op verzoek van een betrokkene een verbetering of verwijdering van persoonsgegevens heeft uitgevoerd, of de verwerking van persoonsgegevens heeft beperkt, zal het bevoegd gezag eventuele ontvangers van de betreffende persoonsgegevens daarover informeren.

Procedure

2. Het bevoegd gezag handelt een verzoek van een betrokkene zo spoedig mogelijk, maar uiterlijk binnen een maand na ontvangst van het verzoek, af. Afhankelijk van de complexiteit en van het aantal verzoeken kan die termijn indien nodig met twee maanden worden verlengd. Als deze verlenging plaatsvindt, wordt de betrokkene daarover binnen een maand na de ontvangst van het verzoek geïnformeerd. Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt. Wanneer het bevoegd gezag geen gevolg geeft aan het verzoek van de betrokkene, deelt het bevoegd gezag onverwijld en uiterlijk binnen een maand na ontvangst mede waarom het verzoek niet wordt ingewilligd en informeert hij de betrokkene over de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens of beroep bij de rechter in te stellen.

Intrekken toestemming

3. Indien voor de verwerking van persoonsgegevens voorafgaande toestemming vereist is, kan deze toestemming te allen tijden door de betrokkene of zijn wettelijk vertegenwoordiger worden ingetrokken. Als de toestemming wordt ingetrokken, staakt het bevoegd gezag de verwerking van persoonsgegevens, behalve als er een andere grondslag (zoals bedoeld in artikel 7) voor de gegevensverwerking is. Het intrekken van de toestemming tast de rechtmatigheid van verwerkingen die reeds hebben plaatsgevonden niet aan.

14. Transparantie

Het bevoegd gezag informeert de betrokkene(n) actief over de verwerking van hun persoonsgegevens, in ieder geval door middel van een laagdrempelige privacyverklaring. In de privacyverklaring wordt in ieder geval de volgende informatie vermeld:
a) de contactgegevens van het bevoegd gezag;
b) de contactgegevens van de functionaris voor gegevensbescherming van het bevoegd gezag;
c) de doeleinden van de gegevensverwerking en de grondslagen voor de verwerking;
d) een omschrijving van de belangen van het bevoegd gezag indien de verwerking wordt gebaseerd op het gerechtvaardigd belang van het bevoegd gezag;
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 het bevoegd gezag 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 geautomatiseerde besluitvorming, vergezeld van nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.
15. Meldplicht datalekken	Een ieder die betrokken is bij een verwerking van persoonsgegevens is verplicht om een datalek per ommegaande te melden bij het meldpunt (avg@lucasonderwijs.nl), conform het protocol beveiligingsincidenten en datalekken van het bevoegd gezag. Een datalek is elke inbreuk waarbij persoonsgegevens zijn vernietigd of verloren, gewijzigd, verstrekt of toegankelijk zijn gemaakt.
16. Klachten	1. Wanneer een betrokkene van mening is dat het doen of nalaten van het bevoegd niet in overeenstemming is met de AVG, dit reglement of (andere) toepasselijke wet- of regelgeving, dan kan een klacht worden ingediend overeenkomstig de binnen het bevoegd gezag geldende klachtenregeling. Een betrokkene kan zich eveneens wenden tot de functionaris voor gegevensbescherming van het bevoegd gezag. 2. Als een klacht naar de mening van betrokkene door het bevoegd gezag niet correct is afgewikkeld, kan hij zich wenden tot de rechter of de Autoriteit Persoonsgegevens.
17. Onvoorziene situatie	Indien zich een situatie voordoet die niet beschreven is in dit reglement, neemt het College van Bestuur van het bevoegd gezag de benodigde maatregelen, en wordt beoordeeld of dit reglement dientengevolge moet worden aangevuld of aangepast.
18. Wijzigingen reglement	1. Dit reglement is na instemming van de Gemeenschappelijke Medezeggenschapsraad (GMR) vastgesteld door het College van Bestuur van het bevoegd gezag. Het reglement wordt gepubliceerd op de website van het bevoegd gezag en de websites van de scholen. Het reglement wordt verder actief onder de aandacht gebracht, bijvoorbeeld door middel van verwijzing in de schoolgids. 2. Het College van Bestuur kan dit reglement wijzigen na instemming van de GMR.
19. Slotbepaling	Dit reglement wordt aangehaald als het privacyreglement van Lucas Onderwijs en treedt in werking op **25 mei 2018.**

Dit protocol is met instemming van de Bureauraad op 17 mei 2018, GMR-VO op 22 mei 2018 en de GMR-PO op 23 mei 2018 tot stand gekomen. Vastgesteld door het College van Bestuur d.d. 24 mei 2018.

Bijlage 8: Vragen uit de DPIA

		Vragenlijst Privacy Impact Assessment *			
		** Bron: handreiking NOREA*			
		Vraag	**Extra informatie**	**Ja / Nee**	**Verhoogd Risico/Actie**
			Extra informatie over situatie of vraag	***Loopt u een verhoogd risico?***	***Bij een verhoogd risico de actie omschrijven***
1	Het type project	Is er sprake van het verwerken van persoonsgegevens?		Nee -> u kunt stoppen. Ja -> Ga verder	
2		Is het duidelijk wie verantwoordelijk is voor de verwerking?	1. Voor en door wie wordt project uitgevoerd; 2. Of er iemand formeel verantwoordelijk is; 3. intern contactpersoon	Ja -> Ga verder. Nee -> U loopt een verhoogd risico	Niet duidelijk wie maatregelen moet treffen en risico's worden niet afgedekt. Bovendien compliance risico wegens wettelijke verplichtingen. Actie: beleid opstellen en intern verantwoordelijke aanstellen.
3		Verwerkt uw organisatie de persoonsgegevens in opdracht en onder verantwoordelijkheid van een andere organisatie?	Is de organisatie bewerker of verantwoordelijke?	Ja -> U kunt stoppen; Nee -> Bepaal wie binnen de organisatie verantwoordelijke is.	
4		Is het duidelijk wie na afloop van het project verantwoordelijk is voor het in stand houden en evalueren van de getroffen maatregelen?	Bijvoorbeeld het periodiek uitvoeren van de PIA	Ja -> Ga verder. Nee -> Risico bestaat dat maatregelen niet meer passen bij de situatie in de toekomst	
5		Is het doel van de verwerking van persoonsgegevens binnen het project voldoende SMART omschreven?	Specifiek, Meetbaar, Acceptabel, Realistisch, Tijdgebonden	Ja -> Ga verder. Nee -> Essentieel voor het maken van keuzes voor de inrichting van gegevensverwerking	Compliance risico omdat het doel niet omschreven is.
		Is er sprake van			
6		a. Gebruik van nieuwe technologie?		Ja -> U loopt verhoogd risico; Nee -> Ga verder naar b.	Verhoogde risico kan bijvoorbeeld zijn: - de impact van uw project op de betrokken en de wijze waarop zij gaan reageren; - kan leiden tot imagoschade, - verstoring van de bedrijfscontinuiteit - acties door handhavers en toezichthouders
7		b. Gebruik van technologie die bij het publiek vragen of weerstand op kan roepen?		Ja -> U loopt verhoogd risico; Nee -> Ga verder naar c.	Verhoogde risico kan bijvoorbeeld zijn: - de impact van uw project op de betrokken en de wijze waarop zij gaan reageren; - kan leiden tot imagoschade, - verstoring van de bedrijfscontinuiteit - acties door handhavers en toezichthouders
8		c. de invoering van bestaande technologie in een nieuwe context?		Ja -> U loopt verhoogd risico; Nee -> Ga verder naar d.	Verhoogde risico kan bijvoorbeeld zijn: - de impact van uw project op de betrokken en de wijze waarop zij gaan reageren; - kan leiden tot imagoschade, - verstoring van de bedrijfscontinuiteit - acties door handhavers en toezichthouders
9		d. (andere) grote verschuivingen in de werkwijze van de organisatie, de manier waarop persoonsgegevens worden verwerkt en/of de technologie die daarbij gebruikt wordt?		Ja -> U loopt verhoogd risico; Nee -> Ga verder naar e.	Verhoogde risico kan bijvoorbeeld zijn: - de impact van uw project op de betrokken en de wijze waarop zij gaan reageren; - kan leiden tot imagoschade, - verstoring van de bedrijfscontinuiteit - acties door handhavers en toezichthouders
10		e. een nieuwe verwerking van persoonsgegevens		Ja -> U loopt verhoogd risico; Nee -> Ga verder naar f.	Risicoprofiel verandert. Voer een compliance-check uit.
11		f. verzamelen van meer of andere persoonsgegevens		Ja -> U loopt verhoogd risico; Nee -> Ga verder naar g.	Risicoprofiel verandert. Voer een compliance-check uit.
12		g. gebruik van persoonsgegevens voor een ander doel		Ja -> U loopt verhoogd risico; Nee -> Op alle vragen 'Nee' geantwoord? U kunt nu stoppen.	Risicoprofiel verandert. Voer een compliance-check uit.
13		Is er naast de Wbp/Europese Verordening veel wet- en regelgeving ten aanzien van persoonsgegevens waar het project mee te maken heeft?	Bijvoorbeeld: - wetgeving (Wwft) - gedragscodes - algemene maatregelen van bestuur - jurisprudentie - internationale aspecten - interne regelgeving		
14		Zijn er veel maatschappelijke belanghebbenden?		Ja -> U loopt een verhoogd risico	Als maatschappelijk belanghebbenden reageren, kan uw project vertraging oplopen. Actie: belanghebbenden in kaart brengen en beleid maken op welke wijze belanghebbenden worden geinformeerd/betrokken.
15		Zijn er veel partijen betrokken?	Leveranciers etc.	Ja -> U loopt een verhoogd risico	Let op dat alle partijen nauwkeurig en zorgvuldig omgaan met de persoonsgegevens.
16		Is er een geschillenregeling of een partij waar de betrokkene terecht kan bij vragen of klachten?		Ja -> Ga verder. Nee -> U loopt een verhoogd risico	Actie: contactpunt maken voor vragen en geschillen en waar mogelijk geschillenregeling. Bijdragen aan verbetering van de voorlichting, het imago en belangenbehartiging.

17		Zijn alle gegevens nodig om het doel te bereiken?	Rekening houden met: - per element vaststellen of het toegevoegde waarde is - kan alleen worden volstaan met ja of nee i.p.v. gegevens; - gebruik maken van andere methoden i.p.v. gegevens	Ja -> Ga verder. Nee -> U loopt een verhoogd risico	Verwerken van zo min mogelijk gegevens verkleind het risico op fouten en hoeft minder te worden onderhouden. Daarbij vergt het niet zoveel capaciteit en opslag in uw systemen.
18		Kan het doel met geanonimiseerde of gepseudonimiseerde gegevens worden bereikt?		Ja -> Ga verder. Nee -> U loopt een verhoogd risico	Actie: nagaan of persoonsgegevens kunnen worden geanonimiseerd of gepseudonimiseerd.
19		Kunnen de gegevens gebruikt worden om het gedrag, de aanwezigheid of presentaties van mensen in kaart brengen en/of beoordelen?	Bijvoorbeeld leerlingvolgsystemen.	Ja -> U loopt een verhoogd risico Nee -> Ga verder	Het risico bestaat dat personen dit gaan zien als een bedreiging voor hun privacy. Ook als gegevens niet voor dit doel worden gebruikt, bestaat het risico dat dit in de toekomst wel gebeurt. Voor invoeren van leerlingvolsysteem/personeelsvolgsysteem is toestemming OR nodig.
		Is sprake van het verwerken van:			
20	De gegevens	Bijzondere gegevens?	Bijvoorbeeld persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, persoonsgegevens betreffende het lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.	Ja -> U loopt een verhoogd risico Nee -> Ga verder	Het verwerken van bijzondere gegevens brengt een verhoogd risico op misbruik met zich mee. Deze gegevens dienen beter beschermd te worden. Het verwerken van deze gegevens is alleen toegestaan onder bepaalde wettelijke voorwaarden. Actie: nagaan of bijzondere persoonsgegevens worden verwerkt, of dit toegestaan is door de AVG en hoe deze worden beveiligd.
21		Uniek identificerende gegevens?	Bijvoorbeeld vingerafdrukken	Ja -> U loopt een verhoogd risico Nee -> Ga verder	Het verwerken van uniek identificerende gegevens brengt een verhoogd risico op misbruik met zich mee. Deze gegevens dienen beter beschermd te worden. Het verwerken van deze gegevens is alleen toegestaan onder bepaalde wettelijke voorwaarden. Actie: nagaan of uniek identificerende gegevens worden verwerkt, of dit toegestaan is door de AVG en hoe deze worden beveiligd.
22		Persoonsnummers	Bijvoorbeeld BSN	Ja -> U loopt een verhoogd risico Nee -> Ga verder	Het verwerken van persoonsnummers brengt een verhoogd risico op misbruik met zich mee. Deze gegevens dienen beter beschermd te worden. Het verwerken van deze gegevens is alleen toegestaan onder bepaalde wettelijke voorwaarden. Actie: nagaan of uniek identificerende gegevens worden verwerkt, of dit toegestaan is door de AVG en hoe deze worden beveiligd.
23		Andere gevoelige gegevens	Bijvoorbeeld financiële gegevens, arbeidsprestaties of gegevens waarvoor een geheimhoudingsplicht geldt.	Ja -> U loopt een verhoogd risico Nee -> Ga verder	Vraagt om betere beveiliging omdat er een risico op misbruik is.
24		Worden gegevens van kwetsbare personen of groepen verwerkt?	Bijvoorbeeld minderjarigen, gehandicapten of gedetineerden	Ja -> U loopt een verhoogd risico Nee -> Ga verder	Kwetsbare personen lopen het risico dat de organisatie een negatief beeld gaat vormen over deze personen. Deze gegevens dienen beter te worden beveiligd en betrokkenen moeten de mogelijkheid hebben zich aan deze verwerking te onttrekken.
25		Omvatten de gegevens gehele of grote delen van de bevolking?		Ja -> U loopt een verhoogd risico Nee -> Ga verder	Deze gegevens dienen beter te worden beveiligd.

26	De betrokken partijen	Zijn er bij het verzamelen en verwerken van de gegevens interne partijen betrokken?	Bijvoorbeeld afdelingen die gebruik maken van de gegevens, gegevens verzamelen of personen die toegang hebben tot de gegevens	Ja -> U loopt een verhoogd risico Nee -> Ga verder	Zorg voor een duidelijke beschrijving van de taken en verantwoordelijkheden van de afdelingen en/of personen met betrekking tot de gegevens.
27		Zijn er bij het verzamelen en verwerken van de gegevens externe partijen betrokken?	Bijvoorbeeld partijen die gebruik maken van de gegevens, de gegevens insourcen of gegevens kopen.	Ja -> U loopt een verhoogd risico Nee -> Ga verder	Hoe meer partijen er zijn betrokken, hoe groter het risico op misbruik of verlies van gegevens. Zorg voor een duidelijk beschrijving van de taken en verantwoordelijkheden van externe partijen met betrekking tot de gegevens. Actie: ga na of alle bewerkersovereenkomsten tussen bewerkers en de verantwoordelijke in orde zijn.
28		Zijn er partijen betrokken die zich niet aan een met Nederland vergelijkbare privacywetgeving hoeven te houden?	Bijvoorbeeld partijen die gegevens verwerken buiten de EER, zoals USA.	Ja -> U loopt een verhoogd risico Nee -> Ga verder	De verantwoordelijke is verantwoordelijk voor de verwerking van deze gegevens buiten de EER. Actie: ga na in hoeverre een adequaat beschermingsniveau wordt geboden door het betreffende land en leg dit contractueel vast.
29		Is verstrekking aan derde partijen in lijn met het doel waarvoor de gegevens zijn verzameld?		Ja -> Ga verder Nee -> U loopt een verhoogd risico	Compliance risico omdat gegevens worden verstrekt aan derden die niet voor dat doel zijn verzameld. De gegevens zijn dus niet geschikt voor dat doel en betrokkenen worden mogelijk geschaad.
30	Verzamelen van gegevens	Worden gegevens verzameld op een manier die privacy gevoelig kan zijn?	Bijvoorbeeld camerasystemen, tracking door cookies of GPS?	Ja -> U loopt een verhoogd risico Nee -> Ga verder	Actie: nagaan of gegevens op een andere manier kunnen worden verzameld.
31		Zijn betrokkenen op de hoogte van het doel van het verzamelen van de gegevens?	Bijvoorbeeld door publiekelijke bekendmaking	Ja -> Ga verder Nee -> U loopt een verhoogd risico	Actie: belangenafweging maken of het doel van de gegevensverzameling opweegt tegen de risico's van de betrokkenen.
32		Is er een wettelijke grondslag om de gegevens te verzamelen?	Bijvoorbeeld toestemming, noodzakelijk voor uitvoering van een overeenkomst, wettelijke verplichting, vervulling van publiekrechtelijke taak of een gerechtvaardigd belang.	Ja -> Ga verder Nee -> U loopt een verhoogd risico	Compliance risico indien grondslag ontbreekt.
33		Verzamelt u gegevens op basis van opt-in of opt-out?	Opt-in: betrokkene heeft toestemming gegeven voor de verwerking Opt-out: betrokkene heeft geen toestemming gegeven, maar kan bezwaar maken.	Ja -> Ga verder Nee -> U loopt een verhoogd risico	Betrokkene dient op de hoogte te zijn van de verwerking en moet bezwaar kunnen maken tegen de verwerking.
34		Kunnen betrokkenen de toestemming intrekken?	Wanneer er sprake is van opt-in	Ja -> Ga verder Nee -> U loopt een verhoogd risico	Actie: betrokkenen de mogelijkheid geven om toestemming in te trekken (systeemtechnisch).
35		Is de impact van het intrekken van de toestemming groot voor de betrokkene?	Bijvoorbeeld wanneer dienstverlening niet kan doorgaan als betrokkene toestemming intrekt.	Ja -> U loopt een verhoogd risico Nee -> Ga verder	Compliance risico: geen sprake van vrije wilsuiting door betrokkene.
36		Weten betrokkenen dat gegevens worden verzameld?	Rekening houden met: - afkomst gegevens - wijze van verzamelen - mogelijkheden waarop betrokkene op de hoogte kan zijn - gebruik van technologie - doel van het gebruik - intern gebruik - extern gebruik - bewaartermijn van gegevens	Ja / Nee	Ja: meldt ook de reden waarom gegevens worden verzameld (ook daar waar geen wettelijke verplichting is). Dit vergroot het vertrouwen van de betrokkene. Nee: het verstrekken van informatie over welke gegevens worden verzameld draagt bij aan de transparantie en wekt vertrouwen bij de betrokkenen.

37	Gebruik van gegevens	Is het gebruik van gegevens in overeenstemming met het doel van het verzamelen?	Rekening houden met: - doel - welke gegevens worden verzameld - bijzondere gegevens? - waar komen gegevens vandaan? - hoe vaak worden gegevens verzameld? - welke wijze worden gegevens verzameld? - welke partijen hebben toegang tot de gegevens?	Ja -> Ga verder Nee -> U loopt een verhoogd risico	Compliance risico: u loopt risico dat de gegevens niet geschikt zijn voor het doel.
38		Worden de gegevens gebruikt voor andere processen of doelen dan ze oorspronkelijk zijn verzameld zijn?		Ja -> U loopt een verhoogd risico Nee -> Ga verder	Het gebruik van gegevens dient in overeenstemming te zijn met het doel.
39		Is de kwaliteit van de gegevens gewaarborgd?	Bijvoorbeeld: updaten van gegevens, toegang tot gegevens en correctie van gegevens.	Ja -> Ga verder Nee -> U loopt een verhoogd risico	Compliance risico: gegevens dienen juist verwerkt te worden om misbruik te voorkomen.
40		Worden beslissingen over betrokkenen genomen op basis van de gegevens?		Ja -> U loopt een verhoogd risico Nee -> Ga verder	Actie: let op dat gegevens een volledig en actueel beeld opleveren wegens de kans op een foutieve beslissing.
41		Is sprake van koppeling, verrijking of vergelijking van gegevens uit verschillende bronnen?		Ja -> U loopt een verhoogd risico Nee -> Ga verder	Gegevens kunnen (in de toekomst) gebruikt worden voor andere doeleinden dan waar zij oorspronkelijk voor zijn verzameld. Let op de bewaartermijnen.
42		Worden de gegevens verspreid binnen de organisatie?		Ja -> U loopt een verhoogd risico Nee -> Ga verder	Zorg voor een duidelijke beschrijving van de taken en verantwoordelijkheden van de afdelingen en/of personen met betrekking tot de gegevens.
43		Worden de gegevens verspreid buiten de organisatie?	Let op de verwachtingen van de betrokkenen.	Ja -> U loopt een verhoogd risico Nee -> Ga verder	Zorg voor een duidelijk beschrijving van de taken en verantwoordelijkheden van externe partijen met betrekking tot de gegevens. Actie: ga na of alle bewerkersovereenkomsten tussen bewerkers en de verantwoordelijke in orde zijn. Ga na of de betrokkene op de hoogte is van de verspreiding.
44		Worden er profielen opgesteld op basis van de gegevens?		Ja / Nee	Ja: het nemen van beslissingen op basis van gegevens kan leiden tot discriminatie van bepaalde groepen. Zorg dat duidelijk is op basis waarvan deze profielen worden opgesteld, welke gegevens worden gebruikt en of gevoelige informatie is af te leiden.
45		Kunnen betrokkenen hun gegevens inzien?	Inzagerecht: gegevens wijzigen of verwijderen.	Ja -> Ga verder Nee -> U loopt een verhoogd risico	Actie: systeemtechnisch in orde maken. Betrokkenen hebben het recht om hun gegevens in te zien alsmede te laten wijzigen, corrigeren en verwijderen (compliance risico).
46	Bewaren	Is er een bewaartermijn vastgesteld?	Let op wettelijke verplichtingen, zoals administratieplicht	Ja -> Ga verder Nee -> U loopt een verhoogd risico	Gegevens mogen niet oneindig worden bewaard (compliance risico).
47		Kunnen de gegevens daadwerkelijk worden verwijderd?		Ja -> Ga verder Nee -> U loopt een verhoogd risico	Compliance risico: gegevens mogen niet oneindig worden bewaard. Actie: gegevens vernietigen wanneer ze niet meer nodig zijn of indien dit niet mogelijk de gegevens anonimiseren.
48	Beveiligen	Is er sprake van een intern beleid over het beveiligen van gegevens?	Rekening houden met: - verantwoordelijkheden - algemene beveiligingsstandaarden - bijzondere of gevoelige gegevens - beveiligingsbeleid	Ja -> Ga verder Nee -> U loopt een verhoogd risico	Actie: intern beleid maken omtrent het beveiligen van gegevens. In beleid opnemen: maatregelen die voor een passende bescherming van gegevens zorgen. Houd hierbij rekening met de Richtsnoeren Beveiliging Persoonsgegevens.
49	Datalek	Zijn er maatregelen omtrent de meldplicht datalekken getroffen?	Bedrijven, overheden en organisaties dienen een datalek - onder bepaalde voorwaarden - te melden aan de Autoriteit Persoonsgegevens en soms aan betrokkenen zelf.	Ja -> Ga verder Nee -> U loopt een verhoogd risico	Actie: maatregelen treffen om gestructureerd en adequeaat invulling te geven aan de meldplicht datalekken. Houd rekening met de Richtsnoeren die de Autoriteit Persoonsgegevens heeft gepubliceerd.
		EINDE			

Bijlage 9: FG taken

- het bestuur, directieleden en medewerkers die persoonsgegevens verwerken informeren en adviseren over de verplichtingen ten aanzien op de wettelijke bepalingen ten aanzien van de verwerking van persoonsgegevens;
- ziet toe op de naleving van de AVG en andere Europese wet en regelgeving of nationale bepalingen ten aanzien van de verwerking van persoonsgegevens;
- het toezien op de naleving van het beleid van de organisatie met betrekking tot de bescherming van persoonsgegevens;
- Het toezien op de naleving van verantwoordelijkheden die in de organisatie zijn belegd en het bewustmaken en opleiden van medewerkers en de betreffende audits;
- Gevraagd en ongevraagd advies geven met betrekking tot de gegevensbeschermingseffectbeoordeling, en toezien of de uitvoering daarvan in overeenstemming is met AVG;
- samenwerken Autoriteit Persoonsgegevens (AP) en optreden als contactpersoon voor de AP voor verband houdende aangelegenheden met betrekking tot de verwerking van persoonsgegevens en indien nodig overleg plegen over andere aangelegenheden die met privacy te maken hebben;
- de FG houdt bij de uitvoering van zijn taken rekening met met de risico's die verbonden zijn aan het gebruik van persoonsgegevens, de aard, de omvang, en met de context en de doelen van het gebruik van die gegevens.

Bijlage 10: 10 – stappenplan AVG

In 10 stappen voorbereid op de AVG

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.

Wat verandert er?
De AVG versterkt de positie van de betrokkenen (de mensen van wie gegevens worden verwerkt). Zij krijgen nieuwe privacyrechten en hun bestaande rechten worden sterker. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De nadruk ligt – meer dan nu – op de verantwoordelijkheid van organisaties om te kunnen aantonen dat zij zich aan de wet houden.

Wat kan ik doen?
Als organisatie kunt u nu alvast stappen ondernemen om straks klaar te zijn voor de AVG. Om u hierbij te helpen, heeft de Autoriteit Persoonsgegevens de 10 belangrijkste stappen voor u op een rijtje gezet. Op autoriteitpersoonsgegevens.nl vindt u de antwoorden op veelgestelde vragen.

Stap 1:Bewustwording

Zorg ervoor dat de relevante mensen in uw organisatie (zoals beleidsmakers) op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op uw huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen. Houd er rekening mee dat de implementatie van de AVG veel kan vragen van de beschikbare menskracht en middelen en begin er daarom op tijd mee.

De Autoriteit Persoonsgegevens (AP) biedt instrumenten die u kunnen helpen om de AVG na te leven, zoals guidelines die zijn opgesteld samen met de andere privacytoezichthouders in Europa.

Bedenk dat de AP uw organisatie sancties kan opleggen van maximaal 20 miljoen euro of 4% van uw wereldwijde omzet als u zich niet aan de nieuwe privacywetgeving houdt.

Stap 2: Rechten van betrokkenen

Onder de AVG krijgen de mensen van wie u persoonsgegevens verwerkt meer en verbeterde privacyrechten. Bereid u daar op voor zodat u op tijd en op de juiste manier op verzoeken reageert.

Denk daarbij aan bestaande rechten, zoals het recht op inzage en het recht op correctie en verwijdering. Maar houd ook alvast rekening met nieuwe rechten, zoals het recht op dataportabiliteit. Bij dit recht moet u ervoor zorgen dat betrokkenen hun gegevens makkelijk kunnen krijgen en vervolgens kunnen doorgeven aan een andere organisatie als ze dat willen.

Ook kunnen mensen bij de AP klachten indienen over de manier waarop u met hun gegevens omgaat. De AP is verplicht deze klachten te behandelen.

Stap 3: Overzicht verwerkingen

Breng uw gegevensverwerkingen in kaart. Documenteer welke persoonsgegevens u verwerkt en met welk doel u dit doet, waar deze gegevens vandaan komen en met wie u ze deelt. Onder de AVG heeft u een verantwoordingsplicht, wat inhoudt dat u moet kunnen aantonen dat uw organisatie in overeenstemming met de AVG handelt.

U kunt het overzicht ook nodig hebben als betrokkenen hun privacyrechten uitoefenen. Als zij u vragen hun gegevens te corrigeren of verwijderen, moet u dit doorgeven aan de organisaties waarmee u hun gegevens heeft gedeeld.

Vermeld in het overzicht ook per categorie van gegevens op basis van welke wettelijke grondslag u deze gegevens verwerkt. Beroept u zich bijvoorbeeld op een gerechtvaardigd belang of vraagt u toestemming aan de betrokkenen? NB: de grondslagen in de AVG zijn grotendeels hetzelfde als die in de huidige Wbp.

Stap 4: Data protection impact assessment

Onder de AVG kunt u verplicht zijn een zogeheten *data protection impact assessment* (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

U moet een DPIA uitvoeren als uw beoogde gegevensverwerking waarschijnlijk een hoog privacyrisico met zich meebrengt. U kunt nu alvast inschatten of u straks DPIA's moet uitvoeren en hoe u dit dan gaat aanpakken.

Komt straks uit een DPIA naar voren dat uw beoogde verwerking een hoog risico oplevert? En lukt het u niet om maatregelen te vinden om dit risico te beperken? Dan moet u met de AP overleggen voordat u met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd. De AP beoordeelt dan of de voorgenomen verwerking in strijd is met de AVG. Is dit het geval, dan ontvangt u een schriftelijk advies van de AP.

Stap5:Privacybydesign&privacybydefault

Maak uw organisatie nu al vertrouwd met de onder de AVG verplichte uitgangspunten van *privacy by design*
en *privacy by default* en ga na hoe u deze beginselen binnen uw organisatie kunt invoeren.

Privacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd.

Privacy by default houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken. Bijvoorbeeld door: een app die u aanbiedt niet de locatie van gebruikers te laten registeren als dat niet nodig is; op uw website het vakje 'Ja, ik wil aanbiedingen ontvangen' niet vooraf aan te vinken; als iemand zich op uw nieuwsbrief wil abonneren niet meer gegevens te vragen dan nodig is.

Stap 6: Functionaris voor de gegevensbescherming

Onder de AVG kunnen organisaties verplicht zijn om een functionaris voor de gegevensverwerking (FG) aan te stellen. Bepaal nu alvast of dit voor uw organisatie geldt. Zo ja, wacht dan niet te lang met het werven van een FG. Uiteraard mag uw organisatie ook vrijwillig een FG aanstellen.

Stap 7: Meldplicht datalekken

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan uw eigen registratie van de datalekken die zich in uw organisatie hebben voorgedaan. U moet alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan. Dit gaat verder dan de huidige protocolplicht uit de Wbp, die alleen betrekking heeft op de gemelde datalekken.

Stap 8:Bewerkersovereenkomsten

Heeft u uw gegevensverwerking uitbesteed aan een bewerker (in de AVG 'verwerker' genoemd)? Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met uw bewerkers nog steeds toereikend zijn en voldoen aan de vereisten in de AVG. Zo niet, breng dan tijdig noodzakelijke wijzigingen aan.

Stap 9: Leidende toezichthouder

Heeft uw organisatie vestigingen in meerdere EU-lidstaten? Of hebben uw gegevensverwerkingen in meerdere lidstaten impact? Dan hoeft u onder de AVG nog maar met één privacytoezichthouder zaken te doen. Dit wordt de leidende toezichthouder genoemd. Geldt dit voor uw organisatie, bepaal dan onder welke privacytoezichthouder u valt.

Stap 10:Toestemming

Voor sommige gegevensverwerkingen hebt u toestemming nodig van de betrokkenen. De AVG stelt strengere eisen aan toestemming. Evalueer daarom de manier waarop u toestemming vraagt, krijgt en registreert. Pas deze wijze indien nodig aan. Nieuw is dat u moet kunnen aantonen dat u geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven.