

DPIA Xedule en My Xedule

Data protection impact assessment op de verwerkingen van persoonsgegevens in Xedule en My Xedule

8 juli 2025

Inhoudsopgave

1	Samenvatting	6
2	Inleiding	13
2.1	Aanleiding	13
2.2	Centrale DPIA door SURF	14
2.3	Model	15
2.4	Methodologie	15
2.5	Scope van deze DPIA	16
2.6	Out of scope	17
A.	Beschrijving algemene kenmerken gegevensverwerkingen	18
3	Introductie Xedule	18
3.1	Toelichting Xedule en My Xedule	18
3.1.1	<i>Xedule</i>	18
3.1.2	<i>My Xedule</i>	18
3.1.3	<i>Proces</i>	19
3.2	Privacy by Design en Privacy by Default	20
4	Verwerkingsdoeleinden	23
4.1	Doelen instellingen (conform HORA)	23
4.1.1	<i>Hoofddoel: Onderwijsplanning</i>	23
4.1.2	<i>Hoofddoel: Roostering</i>	24
4.2	Aanvullende verwerkingsdoeleinden	25
5	Persoonsgegevens	26
6	Gegevensverwerkingen	28
6.1	Roosteren & plannen van onderwijs	28
6.1.1	<i>Geautomatiseerde verzameling</i>	28
6.1.2	<i>Handmatige verzameling</i>	30
6.1.3	<i>Opslag</i>	36
6.1.4	<i>Datamanagement</i>	36
6.1.5	<i>Publiceren</i>	37
6.1.6	<i>Verwijdering van gegevens</i>	38
6.2	Beheer	39
6.2.1	<i>Identiteits- en toegangsbeheer</i>	39
6.2.2	<i>Configuratie</i>	41
6.3	Logging	41
6.3.1	<i>Applicatielogging</i>	42
6.3.2	<i>Systeemlogging</i>	43
6.4	Inzageverzoeken	45

7	Technieken en methoden van de gegevensverwerkingen	47
7.1	Software-as-a-Service	47
7.2	Geautomatiseerde besluitvorming	47
7.3	Backup	47
7.4	Pseudonimiseren	48
7.5	Anonimiseren / pseudonimiseren	48
7.6	Encryptie	48
7.6.1	<i>Encryptie data in transit</i>	48
7.6.2	<i>Encryptie data at rest</i>	49
7.7	API's	49
7.7.1	<i>Gestandaardiseerde integratiemogelijkheden</i>	49
7.7.2	<i>Delen</i>	50
7.8	Cookies	53
7.8.1	<i>Xedule</i>	53
7.8.2	<i>My Xedule</i>	53
8	Betrokken partijen	55
8.1	Onderwijsinstelling: Verwerkingsverantwoordelijke	55
8.2	Xedule: Verwerker	56
8.3	Xedule: Verwerkingsverantwoordelijke	56
8.3.1	<i>Verbeteren van dienstverlening en applicatie</i>	56
8.3.2	<i>Systeemlogging voor betrokkeneverzoeken, foutanalyses en analyses rondom informatiebeveiliging en datalekken</i>	57
8.3.3	<i>Marketing en communicatie</i>	58
8.4	Subverwerkers van Xedule	58
8.5	Betrokkenen	60
8.6	Ontvangers	60
8.7	Verstrekkers	60
8.8	Derden	60
9	Belangen bij de gegevensverwerkingen	62
9.1	Onderwijsinstelling	62
9.2	Studenten	62
9.3	Medewerkers (Docenten)	63
9.4	Xedule	63
10	Verwerkingslocaties	64
11	Juridisch en beleidsmatig kader	65
11.1	Juridische en beleidsmatige kaders	65
11.2	Corporate Xedule beleid	66
12	Bewaartermijnen	67
12.1	Bewaartermijnen als verwerker	67
12.2	Bewaartermijnen als verwerkingsverantwoordelijke	68

B. Beoordeling rechtmatigheid gegevensverwerkingen	69
13 Rechtsgrond	69
13.1 Grondslagen instellingen	69
13.2 Grondslagen Xedule	70
13.2.1 Verbeteren van dienstverlening en applicatie	71
13.2.2 Fraudepreventie en beveiliging	71
13.2.3 Marketing en communicatie	72
14 Bijzondere persoonsgegevens	73
14.1 Medewerkers	73
14.2 Studenten	73
15 Doelbinding	75
15.1 Interne doelbinding	75
15.2 Doelbinding Xedule	75
16 Noodzaak en evenredigheid	76
16.1 Subsidiariteit	76
16.2 Proportionaliteit	77
17 Rechten van de betrokkenen	79
C. Beschrijving en beoordeling risico's voor betrokkenen	81
18 Risico's voor betrokkenen	81
18.1 Verlies van controle door Xedule als verwerkingsverantwoordelijke	82
18.2 Verlies van controle door gebrek aan transparantie logging, pNPS en marketing	82
18.3 Verlies van vertrouwelijkheid en sociaal nadeel door te brede definiëring afwezigheids- en hulpmiddelencategorieën	83
18.4 Niet mogelijk om AVG-rechten uit te oefenen en verlies van controle door gebrek aan transparantie subverwerkers	83
18.5 Verlies van vertrouwelijkheid door doorgeven beschikbaarheidsredenen aan roosteraars	84
18.6 Verlies van controle en vertrouwelijkheid door overige vrije velden	84
18.7 Gemiste kansen en verlies van vertrouwelijkheid door handmatige invoer	85
18.8 Verlies van controle en vertrouwelijkheid door niet automatisch te configureren bewaartermijnen	85
18.9 Niet uit kunnen oefenen van AVG-rechten door incomplete inzageverzoeken	86

18.10	Verlies van controle en vertrouwelijkheid door het niet hebben van automatische import/export	86
18.11	Verlies van controle en vertrouwelijkheid door tabellen	87
18.12	Verlies van vertrouwelijkheid door handmatige RBAC	87
18.13	Verlies van vertrouwelijkheid door onduidelijke configuratiewijzigingen	87
18.14	Verlies van vertrouwelijkheid door Xedule rest API	88
18.15	Verlies van vertrouwelijkheid en controle door ongeautoriseerde toegang door verouderde SOAP API	88
18.16	Heridentificering van gepseudonimiseerde gegevens door gebrekkige anonimiseringsmethode	88
18.17	Heridentificering gepseudonimiseerde pNPS-gegevens	89
18.18	Verlies van vertrouwelijkheid door door ontbreken 'read access logging'	90
D. Beschrijving voorgenomen maatregelen		91
19 Maatregelen		91
Conclusie		103
20 Bijlage 1: Resultaten technische analyse		104
20.1	Onderschepte data	104
20.2	Test scenario's	106
20.3	Voorbeeld inzageverzoek	111
21 Bijlage 2: persoonsgegevens		114
22 Bijlage 3: MORA vergeleken met HORA		116
Voor deze verwerking relevante processen beschreven in HORA		117
	<i>Onderwijsplanning</i>	117
	<i>Roosteren</i>	118
Voor deze verwerking relevante processen beschreven in MORA		118
	<i>Plannen en Roosteren</i>	118
	<i>Prognosticeren mensen- en middelen behoefte</i>	121

1 Samenvatting

Dit rapport is een data protection impact assessment (hierna: DPIA) over het gebruik van de SaaS-applicaties Xedule en My Xedule door Nederlandse onderwijs- en onderzoeksinstituten (hierna: instellingen), aangeboden door Xedule B.V. (voormalig Xedule Advitae B.V.; hierna: Xedule). Deze DPIA is een centrale DPIA, uitgevoerd door sectororganisatie SURF, die de instellingen een algemeen kader biedt voor het beoordelen van gegevensbeschermingsrisico's binnen Xedule en My Xedule.

Scope

Xedule en My Xedule ondersteunen instellingen onder andere bij het opstellen en beheren van roosters van medewerkers en studenten en het maken van de inzet- en middelenplanning. Xedule is hierbij de plan- en roosterapplicatie voor het onderwijs en ondersteunt het onderwijslogistieke proces van instellingen, van het maken van dagroosters tot meerjarenplanningen. Daarnaast is Xedule het bronsysteem voor My Xedule: het bijbehorende selfserviceplatform van Xedule. My Xedule maakt het mogelijk om de door de roosteraars in Xedule opgestelde roosters van de medewerkers en studenten te tonen.

De DPIA heeft de plan- en roosterverwerkingen in Xedule en My Xedule in kaart gebracht door middel van documentatieonderzoek en door het uitvoeren van use case scenario's in de applicaties zelf. SURF heeft vervolgens een inzageverzoek ingediend bij Xedule om inzicht te krijgen in welke verwerkingen van persoonsgegevens, waaronder logging en telemetrie, er plaatsvinden bij het uitvoeren van deze scenario's. Ook heeft er een technische analyse plaatsgevonden om inzicht te krijgen of de geobserveerde gegevensverwerkingen overeenkwamen met de documentatie. Aan de hand van dit onderzoek beoordeelt de DPIA of er risico's voor de rechten en vrijheden voortvloeien uit de gegevensverwerkingen in en omtrent Xedule en My Xedule.

AVG-rollen

Xedule treedt voornamelijk op als verwerker voor de verwerkingen in Xedule en My Xedule ten behoeve van de plan- en roosterdoelen van de instellingen en heeft hiervoor ook verwerkersovereenkomsten met haar klanten. Tijdens de DPIA is echter gebleken dat Xedule ook verwerkingen uitvoert die buiten deze overeenkomsten vallen, waaronder logging.

Resultaat en conclusie

Deze DPIA heeft geconstateerd dat er zeventien hoge risico's en één middenrisico zijn bij het gebruik van Xedule en My Xedule. De voornaamste oorzaken van deze risico's zijn:

- Een gebrek aan transparantie van Xedule over verwerkingen die het bedrijf onder eigen verantwoordelijkheid uitvoert;

- Onvoldoende reactie op SURFs inzageverzoek;
- Gebrekkige overeenkomsten met subverwerkers;
- Configuratiekeuzes in de applicaties die niet in lijn zijn met privacy by design en privacy by default.

Xedule heeft echter voldoende handelingsperspectief geboden op het implementeren van de benodigde maatregelen om deze risico's te mitigeren. Daarom zal SURF in 2026 het onderzoek opnieuw uitvoeren en een bijgewerkte versie van de DPIA publiceren. Voorlopig kan het gebruik van Xedule en My Xedule worden voortgezet.

Verlies van controle door Xedule als verwerkingsverantwoordelijke						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	
18.1	Xedule als verwerkersverantwoordelijke, waardoor instellingen geen instructies over verwerkingen kunnen geven	Verlies van controle instellingen	Waarschijnlijk	Zwaar	Hoog	Huidig risico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	Restrisico
		Juridisch en feitelijk de rol van verwerker aannemen voor alle verwerkingen waarbij instellingen Xedule geen toestemming geven voor verdere verwerking als verwerkingsverantwoordelijke	Laag	Zwaar	Laag	

Verlies van controle door gebrek aan transparantie logging, pNPS en marketing						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risico-score	
18.2	Gebrek aan transparantie over gegevensverwerkingen door Xedule	Verlies van controle over onder andere systeemloggingsgegevens	Waarschijnlijk	Zwaar	Hoog	Huidig risico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risico-score	Restrisico
		Inzage verschaffen in alle verwerkingen bij inzageverzoeken	Minimaal	Zwaar	Laag	
		Inzicht bieden in loggingpraktijken in complete en up-to-date documentatie, bijvoorbeeld een loggingbeleid				
		Feitelijke loggingpraktijken laten aansluiten bij				

		gedocumenteerde loggingpraktijken				
		Inzicht bieden in pNPS-verwerkingen				

Verlies van vertrouwelijkheid en sociaal nadeel door te brede definiëring afwezigheids- en hulpmiddelencategorieën

Referentie	Aanleiding	Gevolg	Kans	Impact	Risico-score	
18.3	Mogelijkheid tot definiëren en verwerken categorieën (bijzondere) persoonsgegevens in pick lists en open velden	Verlies van vertrouwelijkheid en sociaal nadeel voor betrokkenen	Redelijk	Zwaar	Hoog	Huidig risico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risico-score	Restrisico
	Duidelijk beleid op de redenen voor afwezigheid die worden geregistreerd	Duidelijke strategie implementeren om klanten en gebruikers (in de context van de verwerking) te waarschuwen categorieën niet te breed te definiëren en geen (bijzondere) persoonsgegevens in open velden op te nemen	Laag	Zwaar	Laag	
	Duidelijke training en instructie over welke gegevens wel en niet in open velden mogen worden geregistreerd					
	Monitoring van de effectiviteit van dit beleid					

Niet mogelijk om AVG-rechten uit te oefenen en verlies van controle door gebrek aan transparantie subverwerkers

Referentie	Aanleiding	Gevolg	Kans	Impact	Risico-score	
18.4	Gebrek aan transparantie subverwerkers	Niet mogelijk om AVG-rechten volledig uit te oefenen voor betrokkenen en verlies van controle instellingen	Waarschijnlijk	Zwaar	Hoog	Huidig risico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risico-score	Restrisico
	Periodieke controle op overzicht subverwerkers	Hoofd- en verwerkersovereenkomsten sluiten met alle subverwerkers met een duidelijke instructie over de te verwerken persoonsgegevens en een lijst met subverwerkers	Laag	Zwaar	Laag	

Verlies van vertrouwelijkheid door doorgeven beschikbaarheidsredenen aan roosteraars						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risico-score	
18.5	Doorgeven beschikbaarheidsredenen aan roosteraars	Verlies van vertrouwelijkheid	Waarschijnlijk	Enige	Hoog	Huidig risico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risico-score	Restrisico
	Implementeer bewaartermijnen voor de motivatie	Mogelijkheid implementeren om beschikbaarheidsredenen te verbergen voor gebruikers die er geen toegang toe nodig hebben voor hun functie	Laag	Enige	Laag	
	Geef duidelijke instructie aan gebruikers wat er wel en niet in de open velden moet worden ingevuld	Duidelijke strategie implementeren om klanten en gebruikers (in de context van de verwerking) te waarschuwen geen (bijzondere) persoonsgegevens in open velden op te nemen				

Verlies van controle en vertrouwelijkheid door overige vrije velden						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	
18.6	Invullen vrije velden	Verlies van controle en vertrouwelijkheid	Redelijk	Zwaar	Hoog	Huidig risico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	Restrisico
	Duidelijke training en instructie over welke gegevens wel en niet in open velden mogen worden geregistreerd	Duidelijke strategie implementeren om klanten en gebruikers (in de context van de verwerking) te waarschuwen geen (bijzondere)	Laag	Zwaar	Laag	
	Monitoring van de effectiviteit van dit beleid	persoonsgegevens in open velden op te nemen				

Gemiste kansen en verlies van vertrouwelijkheid door handmatige invoer						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	
18.7	Handmatige invoer van verkeerde informatie	Gemiste lessen en gemiste kansen om ingeroosterd te worden	Redelijk	Enige	Midden	Huidig risico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	Restrisico
	Training roosteraars	-	Laag	Enige	Laag	

	Automatiseren invoer waar mogelijk					
--	------------------------------------	--	--	--	--	--

Verlies van controle en vertrouwelijkheid door niet automatisch te configureren bewaartermijnen						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	Huidig risico
18.8	Geen automatische bewaartermijnen	Verlies van controle en vertrouwelijkheid	Hoog	Hoog	Hoog	
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	Restrisico
	Vaststellen en beheren bewaartermijnen persoonsgegevens	Technische configuratie en beheer van bewaartermijnen per groep persoonsgegevens faciliteren	Laag	Hoog	Laag	
	Naleving bewaartermijnen vastleggen in processen	Inzichtelijk maken procedure verwijderen persoonsgegevens door middel van een verzoek aan Xedule				

Niet uit kunnen oefenen van AVG-rechten door incomplete inzageverzoeken						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	Huidig risico
18.9	Incomplete inzageverzoeken	AVG-rechten niet kunnen uitoefenen	Waarschijnlijk	Zwaar	Hoog	Huidig risico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	Restrisico
		Volledige inzage in verwerkingen verschaffen bij een inzageverzoek, bijvoorbeeld door beheerders de mogelijkheid te bieden zelf inzage te krijgen of door een duidelijke procedure te implementeren om inzageverzoeken te verwerken	Laag	Zwaar	Laag	

Verlies van controle en vertrouwelijkheid door het niet hebben van automatische import/export						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risico-score	
18.10	Handmatige import/export	Verlies van controle en vertrouwelijkheid	Redelijk	Zwaar	Hoog	Huidig risico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risico-score	Restrisico
	Waar mogelijk automatische koppeling met bronsystemen maken	Optie van automatisch import/export uitlichten en aanraden waar mogelijk	Laag	Zwaar	Laag	
	Duidelijke training en instructie voor degenen die gebruik moeten maken van handmatige import/export	Automatische import/export faciliteren waar mogelijk				

Verlies van controle en vertrouwelijkheid door tabellen						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	
18.11	Configuratie van tabellen waardoor kopiëren en exporteren mogelijk is	Verlies van controle en vertrouwelijkheid	Redelijk	Zwaar	Hoog	Huidig risico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	Restrisico
	Duidelijke instructie voor gebruikers dat er geen gegevens geëxporteerd mogen worden, tenzij hier een goede (van tevoren bepaalde) reden voor is	Configuratiemogelijkheden bieden om de optie om gegevens uit tabellen te kopiëren en exporteren gericht uit te schakelen	Laag	Zwaar	Laag	

Verlies van vertrouwelijkheid door handmatige RBAC						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	
18.12	Alleen handmatige RBAC in applicaties	Verlies van vertrouwelijkheid	Redelijk	Zwaar	Hoog	Huidig risico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	Restrisico
	Richt processen in voor beheren van rollen en monitor de implementatie daarvan (RBAC)	Ondersteun een geautomatiseerde koppeling met externe identiteits- en toegangsbeheersystemen	Laag	Zwaar	Laag	
	Implementeer een centraal systeem voor beheren rechten					

Kans op vertrouwelijkheid door onduidelijke configuratiewijzigingen						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	
18.13	Onduidelijke configuratiewijzigingen	Verlies van controle en vertrouwelijkheid	Redelijk	Zwaar	Hoog	Huidig risico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	Restrisico
	Maak deze instellingen alleen beschikbaar aan medewerkers die training hebben gehad over het gebruik ervan	Richt de interface op een manier die onbewuste autorisatiefouten tegengaat, bijvoorbeeld door visueel duidelijk te maken voor gebruikers welke autorisatiewijzigingen er zijn doorgevoerd	Laag	Zwaar	Laag	

Verlies van vertrouwelijkheid door Xedule rest API						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	
18.14	Toegang zonder onderscheid door Xedule rest API	Verlies van controle en vertrouwelijkheid	Redelijk	Zwaar	Hoog	Huidig risico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	Restrisico
	Geef andere systemen alleen de minimaal	Wijzig het autorisatiemodel van de API, zodat de toegang	Laag	Zwaar	Laag	

	benodigde toegang tot persoonsgegevens in de applicaties	door een ander systeem tot een dataset beperkt kan worden tot de minimaal benodigde set				
--	--	---	--	--	--	--

Verlies van vertrouwelijkheid en controle door ongeautoriseerde toegang door verouderde SOAP API						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	Huidig risico
18.15	Ongeautoriseerde toegang door verouderde SOAP API	Verlies van controle en vertrouwelijkheid	Redelijk	Zwaar	Hoog	Huidig risico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	Restrisico
	De SOAP API koppeling uitfasen	Ondersteuning van de SOAP API uitfasen	Laag	Zwaar	Laag	

Heridentificering van gepseudonimiseerde gegevens door gebrekkige anonimiseringsmethode						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	Huidig risico
18.16	Onjuiste anonimiseringsmethode	Heridentificering betrokkenen	Redelijk	Zwaar	Hoog	Huidig risico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	Restrisico
	AVG-waARBorgen toepassen op door Xedule gepseudonimiseerde persoonsgegevens	In de dienstverlening duidelijk maken dat het om pseudonimisering gaat	Laag	Midden	Laag	

Heridentificering gepseudonimiseerde pNPS-gegevens						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	Huidig risico
Fout! Verwijzingsbron niet gevonden.	Onduidelijkheid over pseudonimiseringsmethoden	Heridentificering persoonsgegevens betrokkenen	Waarschijnlijk	Enige	Hoog	Restrisico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	
	Maak gebruik van de opt-out zolang er geen opt-in mechanisme is	Verander het mechanisme naar opt-in	Laag	Enige	Laag	
		Implementeer aantoonbare maatregelen om heridentificatie te voorkomen				

Verlies van vertrouwelijkheid door door ontbreken 'read access logging'						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	Huidig risico
18.18	Ontbreken read access logging	(Verder) verlies van vertrouwelijkheid	Waarschijnlijk	Zwaar	Hoog	Huidig risico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	Restrisico
	Gebruik maken van de read access logs wanneer nodig	Read access logging implementeren	Laag	Zwaar	Laag	

2 Inleiding

Xedule is een organisatie van Nederlandse origine, gespecialiseerd in het ontwikkelen van onderwijslogistieke software. Hiermee voorziet Xedule in de behoefte van een proces op het gebied van formatie, plannen en roosteren. Xedule heeft twee softwarepakketten die zij sectorbreed aanbieden: Formatie (Foleta) en Xedule. Formatie (Foleta) wordt enkel aangeboden aan het primair onderwijs (hierna: po) en voortgezet onderwijs (hierna: vo) en valt daarmee buiten de scope van deze DPIA.

Het softwarepakket Xedule, inclusief My Xedule, wordt aangeboden aan het middelbaar beroepsonderwijs (hierna: mbo), het hoger beroepsonderwijs (hierna: hbo) en het wetenschappelijk onderwijs (hierna: wo). Dit softwarepakket ondersteunt instellingen onder andere bij het opstellen en beheren van roosters van medewerkers en studenten, het maken van de inzet- en middelenplanning, het optimaliseren van het gebruik van ruimtes en faciliteiten van de instellingen en het aanbieden van gepersonaliseerd flexibel onderwijs.

Een groot aantal instellingen maakt al gebruik van Xedule. Vanuit het oogpunt van een zorgvuldige omgang met persoonsgegevens is het bestuur van een onderwijsinstelling als verwerkingsverantwoordelijke gehouden om te onderzoeken of persoonsgegevens onder hun beheer zorgvuldig en veilig worden verwerkt (intern, maar ook door externe partijen).

2.1 Aanleiding

Instellingen kunnen de wettelijke verplichting hebben om een gegevensbeschermingseffectenbeoordeling ofwel een Data Protection Impact Assessment (hierna: DPIA) uit te voeren. Conform artikel 35 van de Algemene Verordening Gegevensverordening (hierna: AVG) is een DPIA vereist voor verwerkingen die waarschijnlijk een verhoogd risico opleveren. Dit is een open norm, maar artikel 35 lid 3 van de AVG noemt enkele voorbeelden van situaties waarin hiervan sprake is: i) grootschalige geautomatiseerde besluitvorming, ii) grootschalige verwerking van bijzondere persoonsgegevens en iii) grootschalige monitoring van het publiek.

Daarnaast zijn er toetsingskaders die aangeven wanneer een DPIA moet worden uitgevoerd. De Autoriteit Persoonsgegevens (hierna: AP) heeft een niet-uitputtende lijst¹ opgesteld van soorten verwerkingen waarvoor het uitvoeren van een DPIA verplicht is. Ook de EDPB² heeft een lijst opgesteld met negen criteria die kunnen bepalen of een verwerking een verhoogd risico oplevert. Indien sprake is van twee of meer criteria van deze twee lijsten, kan een verwerkingsverantwoordelijke ervan uitgaan dat een DPIA moet worden uitgevoerd.

¹ <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/data-protection-impact-assessment-dpia>, geraadpleegd op 12 juni 2025.

² Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679.

De onderwijssector kent omstandigheden die specifieke uitdagingen met zich meebrengen, waardoor extra zorgvuldigheid en aandacht ten aanzien van de omgang met persoonsgegevens vereist is. Zo kunnen instellingen te maken hebben met studentenpopulaties met uiteenlopende achtergronden, situaties of kwetsbaarheden die de gevoeligheid van de gegevensverwerkingen vergroten. (nummer 7 EDPB-lijst: Gegevens over kwetsbare personen) Daarnaast verwerken instellingen gegevens van al hun studenten en docenten in Xedule. Er zijn honderdduizenden studenten in Nederland. De groep betrokkenen waarvan persoonsgegevens verwerkt kunnen worden is dus relatief per instelling en in zijn totaliteit groot. (nummer 5 EDPB-lijst: Grootschalige verwerkingen) Ook is er een reële mogelijkheid dat instellingen gezondheidsgegevens verwerken om hun planningen en roosters op te stellen. (nummer 4 EDPB-lijst: Gevoelige gegevens) Er is dus voldoende aanleiding om een DPIA uit te voeren op Xedule en My Xedule. Om die reden is er ten behoeve van de leden van SURF³ een DPIA uitgevoerd op Xedule en My Xedule om de risico's voor de privacy van gebruikers te identificeren, beperken en passende maatregelen te nemen om de persoonsgegevens onder de verantwoordelijkheid van instellingen te beschermen.

Verzoek DPIA door Xedule

Noemenswaardig is dat Xedule op eigen initiatief SURF heeft benaderd met het verzoek om een DPIA op Xedule en My Xedule uit te voeren. Dit verzoek toont niet alleen een proactieve benadering, maar onderstreept ook haar welwillendheid tot een constructieve samenwerking. Dit getuigt van inzicht in het belang van een grondige DPIA en het streven om gezamenlijk zorg te dragen voor een aantoonbaar veilig en verantwoord product.

2.2 Centrale DPIA door SURF

Deze DPIA is uitgevoerd door SURF, de ict-coöperatie van Nederlandse onderwijs- en onderzoeksinstituten. SURF voert ten behoeve van de instellingen compliance assessments uit op leveranciers die technologische oplossingen aanbieden binnen de onderwijssector, waaronder DPIA's. De verwerkingsverantwoordelijke voor de verwerkingen die in deze DPIA beoordeeld worden is dus niet SURF, maar de instellingen die gebruik maken van Xedule en My Xedule. De DPIA is dan ook een 'centrale' of 'overkoepelende' DPIA, en biedt de instellingen een algemeen kader voor het beoordelen van gegevensbeschermingsrisico's binnen Xedule en My Xedule. Hiermee geeft de sector gezamenlijk invulling aan wettelijke verplichtingen.

Door het bundelen van expertise realiseert SURF kostenbesparing, kennisdeling en heeft SURF namens de onderwijs- en onderzoekssector een sterkere onderhandelingspositie richting de leveranciers ten aanzien van het nemen van eventuele mitigerende maatregelen. Dit levert voor de leverancier het voordeel op dat deze niet hetzelfde DPIA-proces met

³ Overzicht leden van SURF | [SURF.nl](https://surf.nl).

iedere klant uit de sector hoeft te doorlopen en in één keer maatregelen kan implementeren die (hoge) risico's voor de hele sector mitigeren. De AP heeft de kracht van de samenwerking van de onderwijs- en onderzoeksinstellingen via SURF onderschreven en benadrukt dat dit wijze bijdraagt aan het beschermen van de persoonsgegevens in het onderwijs en onderzoek.⁴

In deze centrale DPIA wordt onderzocht hoe de persoonsgegevens van studenten en medewerkers van de instellingen binnen Xedule en My Xedule worden verwerkt, welke centrale afspraken er zijn gemaakt over de verwerkingen, welke risico's er bestaan en welke maatregelen genomen kunnen worden om deze risico's te beperken. De DPIA biedt een startpunt, maar is op zichzelf staand niet voldoende om als verwerkingsverantwoordelijke aantoonbaar te voldoen aan de AVG. Het door de onderwijsinstelling uitvoeren van een lokale DPIA is noodzakelijk om organisatiespecifieke risico's in kaart te brengen, passende maatregelen te nemen en verantwoording af te leggen over de verwerkingen. Een lokale DPIA biedt de nodige diepgang en inzichten op specifieke omstandigheden of organisatorische kenmerken die deze centrale DPIA niet kan leveren.

2.3 Model

Deze DPIA is gebaseerd op de model DPIA Rijksdienst.⁵ Dit model sluit goed aan op de werkzaamheden van onderwijs- en onderzoeksinstellingen, die ze in het publieke belang uitvoeren. Aangezien dit een centrale DPIA is, zijn er waar nodig wijzigingen aangebracht in de structuur van het originele model.

Het model bestaat uit vier onderdelen. Onderdeel A behandelt de feiten van de gegevensverwerkingen. Onderdeel B beoordeelt de rechtmatigheid van de behandelde feiten uit onderdeel A. Onderdeel C gaat over risico's voor de rechten en vrijheden van betrokkenen en onderdeel D gaat over de beoogde maatregelen om die risico's aan te pakken.

2.4 Methodologie

Deze DPIA is tot stand gekomen door een combinatie van documentatieonderzoek, technisch onderzoek en toelichting van Xedule naar aanleiding van vragen.

Het documentatieonderzoek bestaat uit het opvragen en analyseren van overeenkomsten, beleidsstukken, procedures en informatiebeveiligingscertificeringen. Ook heeft Xedule de kans gekregen om te reageren op bevindingen, doordat er gerichte vervolgvragen zijn gesteld. Dit deel van het onderzoek is voornamelijk gefocust op welke juridische afspraken

⁴ Zie ook: Sectorbeeld Onderwijs 2021-2023, 24 January 2024, p. 5-6,

<https://www.autoriteitpersoonsgegevens.nl/documenten/sectorbeeld-onderwijs-2021-2023>.

⁵ <https://www.kcbr.nl/sites/default/files/2023-09/Model%20DPIA%20Rijksdienst%20v3.0.pdf>, geraadpleegd op 30 april 2025.

er zijn vastgelegd met betrekking tot de verwerkingen in Xedule en My Xedule. De resultaten van het documentatieonderzoek zijn door de hele DPIA terug te vinden, met een zwaartepunt bij hoofdstuk 8.

Het technische onderzoek binnen de DPIA analyseert de technische aspecten van Xedule en My Xedule. Dit onderzoek sluit aan bij de juridische bevindingen en onderzoekt hoe gegevens worden verzameld, verwerkt, opgeslagen, gedeeld en beveiligd. Door technische analyse van datastromen, opslagmethoden, logging, beveiligingsmaatregelen en privacy-instellingen wordt beoordeeld of de technische implementatie voldoet aan AVG-vereisten. Ook wordt de technische documentatie onderzocht en worden er op dit vlak vragen gesteld aan Xedule. Hoofdstuk 6 gaat in meer detail in op de manieren waarop is getracht inzicht te krijgen in de technische aspecten van de verwerkingen.

2.5 Scope van deze DPIA

Xedule biedt diverse diensten en SaaS-oplossingen aan die gericht zijn op onderwijslogistiek voor verschillende onderwijsniveaus in Nederland:

- (i) Software-as-a-Service (SaaS)-oplossingen:
 - a) Foleta: de applicatie voor formatieplanning, les- en taaktoedeling, voor po en vo.
 - b) Xedule: het plan- en roosterapplicatie voor mbo en ho, inclusief bijbehorende applicatie My Xedule.
- (ii) Adviesdiensten:
 - a) Advisering over plan- en roosterprocessen, onderwijslogistiek en optimalisatie van administratieve processen in het onderwijs.
- (iii) Professionele dienstverlening:
 - a) Tijdelijke inzet van Xedule-professionals bij instellingen.
 - b) Ondersteuning bij implementatie en gebruik van de software.
 - c) Training en opleiding voor gebruikers.

Daar enkel (de basisinrichting van) de SaaS-oplossing onderwerp is van deze DPIA vallen de Adviesdiensten en Professionele Dienstverlening derhalve buiten de scope. De scope van deze DPIA omvat en beperkt zich enkel tot de technologische oplossing aangeboden aan het mbo, hbo en wo:

- i) Software-as-a-Service (SaaS)-oplossing: Xedule, de plan- en roosterapplicatie, inclusief bijbehorende applicatie My Xedule.
- ii) Koppeling / interfaces van en naar Xedule.

Daarnaast is het goed om te benoemen dat deze DPIA een momentopname is. De DPIA vindt plaats aan de hand van de dienstverlening, zoals Xedule die op dit moment aanbiedt. Wijzigingen in de dienstverlening en/of overeenkomst(en) kunnen invloed hebben op de uitkomst van de lokale DPIA.

2.6 Out of scope

Zoals in de vorige alinea te zien is, vallen alle andere SaaS-oplossingen en diensten buiten de scope en worden deze niet meegenomen in deze DPIA. Deze DPIA zal niet ingaan op verwerkingen buiten Xedule of My Xedule, zoals andere tools en/of software waarmee Xedule kan worden geïntegreerd. Denk hierbij aan verwerkingen binnen een personeels-informatiesysteem (hierna: HR-systeem) of een studentinformatiesysteem (hierna: SIS) van een onderwijsinstelling. De DPIA beoordeelt ook Xedules websites en supportwerkzaamheden niet.

Daarnaast heeft SURF parallel aan deze DPIA een security audit uitgevoerd op Xedule aan de hand van de SURF security baseline. Die resultaten zijn niet geïntegreerd in deze DPIA. Er is tijdens het DPIA-onderzoek wel aan gerefereerd om te controleren of er geen tegenstrijdigheden waren tussen de resultaten van de DPIA en de audit. Af en toe zijn de onderdelen van de audit die mogelijk relevant voor de DPIA ook gebruikt als naslagwerk.

A. Beschrijving algemene kenmerken gegevensverwerkingen

3 Introductie Xedule

Een groot aantal⁶ mbo- en hbo-instellingen maakt gebruik van Xedule en My Xedule. Hoewel Xedule op het eerste gezicht in de basis een minder risicovolle applicatie lijkt, is de omgang met persoonsgegevens sterk afhankelijk van de context. Bepaalde instellingen kenmerken zich namelijk door diverse studentenpopulaties met uiteenlopende achtergronden, situaties of kwetsbaarheden waarin een verhoogde behoefte aan begeleiding bestaat, die de gevoeligheid van de roosters vergroten. Onbevoegde inzage in roosters door derden kan schadelijke gevolgen hebben. Denk aan situaties waarin een onbevoegde partij misbruik maakt van roosterinformatie om studenten of medewerkers te benaderen en de veiligheid van de betrokkenen in het geding kan komen door de voorspelbaarheid van hun aanwezigheid op specifieke locaties. Dit zijn uiteraard zeer onwenselijke situaties. Om dergelijke risico's in kaart te brengen wordt deze DPIA uitgevoerd.

3.1 Toelichting Xedule en My Xedule

Xedule en My Xedule zijn twee gescheiden systemen, elk met een eigen koppelingsmechanisme (Application Programming Interface (hierna: API)), eigen database en eigen beveiligingsinfrastructuur. De verwerking van persoonsgegevens vindt gescheiden van elkaar plaats in deze afzonderlijke systemen. Daarmee is het van belang om eerst het onderscheid tussen Xedule en My Xedule te duiden.

3.1.1 Xedule

Xedule is een plan- en roosterapplicatie voor het onderwijs en wordt volledig als SaaS-oplossing geleverd. Deze applicatie ondersteunt het onderwijslogistieke proces van een dagrooster tot een meerjarenplanning. Xedule koppelt (niet-)onderwijstaken aan (de beschikbaarheid van) medewerkers en maakt en beheert daarmee de roosters. Xedule is daarmee de aanleverende bron voor het roosterbureau van de onderwijsinstelling. Xedule biedt ter ondersteuning van de onderwijslogistieke processen diverse mogelijkheden om data te integreren in en te ontsluiten naar andere systemen, alsmede het genereren van rapportages.

3.1.2 My Xedule

De bijbehorende applicatie van Xedule is het selfservice platform: My Xedule. My Xedule maakt het mogelijk om de door de roosteraars in Xedule opgestelde roosters van de

⁶ Bron: Gebruikersgroep Xedule - MBO Digitaal.

medewerkers en studenten te tonen (publiceren). Studenten krijgen middels My Xedule de regie over hun eigen leerproces door eigen roosters te raadplegen, zichzelf in te schrijven voor lessen, toetsen en examens, om werkruimtes en/of lokalen te reserveren, zichzelf in te schrijven op toetsen en examens, maar kunnen ook online of fysieke afspraken met docenten en/of medestudenten inplannen. Naast studenten krijgen ook medewerkers beschikking over het selfservice platform My Xedule. Binnen My Xedule kunnen medewerkers onder andere het plan van inzet en het rooster inzien, hun beschikbaarheid doorgeven of een ruimte reserveren. Ook kunnen gebruikers afspraken met docenten en/of medestudenten plannen.

Goed om te benoemen is dat Xedule de bron is voor My Xedule: My Xedule kan niet functioneren zonder Xedule. Andersom is het voor Xedule zeer goed mogelijk om te functioneren zonder My Xedule. Met de juiste koppeling kan het in Xedule gegenereerde rooster ook getoond worden in eigen platformen van instellingen of persoonlijke agenda's via iCal.

3.1.3 Proces

In Xedule worden doorgaans gewone persoonsgegevens van studenten en medewerkers verwerkt. Enkele voorbeelden hiervan zijn de contactgegevens, roosterinformatie en beschikbaarheid. Naast gewone persoonsgegevens, kunnen er ook bijzondere persoonsgegevens worden verwerkt. Dit zal, evenals het complete overzicht van te verwerken persoonsgegevens, aan bod komen in hoofdstuk 0.

Voor het maken en het tonen van roosters in My Xedule worden applicaties (hierna: bronsystemen) met onderwijslogistieke gegevens, waaronder persoonsgegevens, gekoppeld met Xedule. Vervolgens worden de relevante (persoons)gegevens uit deze bronsystemen geëxtraheerd en als kopie ingelezen en opgeslagen in Xedule. Xedule verwerkt vervolgens deze grootschalige persoonsgegevens van diverse gebruikers om tot een rooster- en/of (meerjaren)planning te komen (back-end). My Xedule publiceert en presenteert de door Xedule gegenereerde roosters op een gebruiksvriendelijke manier aan studenten en medewerkers. Zie hieronder de tabel die het proces overzichtelijk weergeeft.

Systeemcontext	Naam	Xedule	My Xedule
	Systeem type	Backend Planning System	Frontend Self-Service Portal
	Hoofdtoepassing	Roostering & Planning Beheer	Rooster Presentatie & Interactie
	Gebruikerscontext	Internal Operations	End-User Interface
Functionele aspecten	Functionaliteiten	Creatie & beheer roosters	Weergave roosters
		Opstellen klassen (student clustering)	Beschikbaarheidsregistratie
		Examenplanning	Vakinschrijving
		Wijzigingsbeheer	Integratie digitale agenda services (push)
		Managementrapportage	-
		Genereren (geautomatiseerde) roosters	-
		Identity & Access Management	-
		Planning inzet en middelen	-
	Gebruikersrollen	Roosteraars	Studenten
		Beheerders	Docenten
		Administratief personeel	Examenbureau
		Helpdeskmedewerkers	Service desk
		Onderwijsontwikkelaar	Onderwijsassistenten
			Staf
Technische aspecten	Data flow	(Bi)directioneel dataverkeer met bronsystemen	(Bi)directioneel dataverkeer met Xedule
		(Bi)directioneel dataverkeer met My Xedule	Integratie digitale agenda services (push)
		Generatie managementinformatie	API
	Systeem integraties	(Bi)directioneel dataverkeer met HR-systemen	(Bi)directioneel dataverkeer met Xedule
		(Bi)directioneel dataverkeer met studie-informatiesystemen	Integratie digitale agenda services (push)
		(Bi)directioneel dataverkeer met My Xedule	-
		Externe exports	-

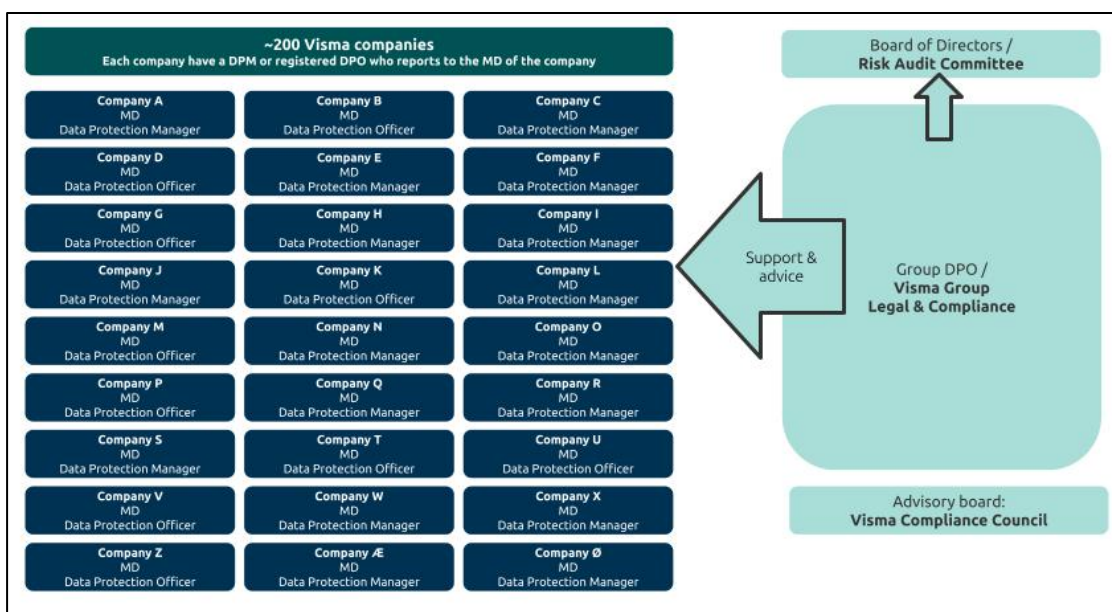
Tabel 3-1, Verschillen tussen Xedule en My Xedule schematisch weergegeven.

3.2 Privacy by Design en Privacy by Default

In de door Xedule aangeleverde documenten is niet expliciet opgenomen dat de beginselen van Privacy by Design en Privacy by Default in Xedule en My Xedule zijn geïmplementeerd. Uit het bureauonderzoek is gebleken dat de rechtsbeginselen omtrent zorgvuldige omgang van persoonsgegevens echter wel stevig verankerd zijn in het centrale beleid van de Visma Group. De Visma Group is het Europese moederbedrijf van ruim 200 Xedule dochterondernemingen, waaronder Xedule B.V.. De Visma Group heeft een overkoepelende strategische rol en algemene kaders en richtlijnen zijn opgesteld voor de dochterondernemingen. Zij kent een gelaagde hiërarchische organisatiestructuur waarin de

dochterondernemingen operationele autonomie hebben, inclusief enige vrijheid in juridische aangelegenheden. Echter, op het gebied van privacy is de autonomie beperkter en moeten de dochterondernemingen voldoen aan de centrale richtlijnen en kaders die zijn opgesteld door de Visma Group⁷. Zo heeft Visma Group een omvangrijk Data Protection Programma en omvat het beleid, richtlijnen, risico- en volwassenheidsmonitoring, incidentafhandeling, bewustwording en alle medewerkers krijgen verplichte privacytrainingen.

Om ervoor te zorgen dat zorgvuldige omgang met persoonsgegevens als onderdeel van de dagelijkse activiteiten en dienstverlening binnen alle dochterondernemingen geborgd is, heeft elke dochteronderneming een Data Protection Manager (DPM) die verantwoordelijk is voor de privacy binnen het bedrijf en rapporteert aan de Managing Director van de dochteronderneming. Het Visma Group Legal & Compliance Team assisteert en adviseert de DPM's in hun dagelijkse werkzaamheden met gegevensbescherming en rapporteert regelmatig aan de Raad van Bestuur via het Risk Audit Committee. De Visma Compliance Council is het adviesorgaan voor Visma Group en haar bedrijven met betrekking tot naleving van EU-wetten en -voorschriften. De AVG krijgt extra aandacht vanwege de aard van Visma Group als softwareleverancier die een groot volume aan persoonlijke gegevens verwerkt en met meer dan 15.000 medewerkers.



Figuur 3-1, Xedule Data Protection Program.

Deze DPIA ziet op een reeds bestaande situatie, aangezien er al gebruik wordt gemaakt van Xedule en My Xedule, en richt zich op de basisinrichting van beide applicaties, alsmede het beschrijven van de huidige situatie. Het uiteindelijke doel is waarborgen dat Xedule en My

⁷ Xedule's [Data Protection Program](#).

Xedule veilig zijn in gebruik en daarnaast een kader bieden voor mogelijke (proces)verbeteringen.

4 Verwerkingsdoeleinden

Xedule verwerkt persoonsgegevens van studenten en medewerkers van instellingen voor verschillende doeleinden. In de verwerkersovereenkomst is het doeleinde “roosteren en plannen van het onderwijs voor studenten en medewerkers” vastgelegd. Dit overkoepelende doeleinde is in paragraaf 4.1 gespecificeerd aan de hand van het HORA-model. Er worden binnen Xedule en My Xedule daarnaast persoonsgegevens verwerkt voor aanvullende doeleinden die niet in de HORA zijn vastgelegd. Op basis van de verwerkersovereenkomst, andere documentatie en analyse van de feitelijke situatie zijn deze aanvullende doeleinden onderscheiden in paragraaf 4.2. In hoofdstuk 8. Betrokken partijen wordt er ingegaan op wie er verantwoordelijk is voor de verwerkingen die plaatsvinden ten behoeve van deze doelen.

4.1 Doelen instellingen (conform HORA)

Xedule, inclusief My Xedule, is een planningstool die wordt gebruikt door instellingen om roosters en planning efficiënt te beheren. Om de doelen beter te duiden en instellingen meer context te bieden, volgt hieronder een opsomming conform het HORA-model.

Het bedrijfsfunctiemodel van de Hoger Onderwijs Referentie Architectuur (HORA)⁸ biedt een gestructureerd overzicht van de bedrijfsfuncties binnen een instelling. Het beschrijft wat een onderwijsinstelling doet, onafhankelijk van de specifieke uitvoering per instelling. Deze DPIA gebruikt dit referentiemodel als basis om de doelen van de gegevensverwerkingen binnen Xedule en My Xedule te beschrijven, zodat ze in lijn zijn met bestaande architecturen en terminologie binnen het onderwijs.⁹ Binnen de doelen uit de HORA is er onderscheid tussen hoofddoelen en subdoelen ten behoeve waarvan de gegevensverwerkingen binnen Xedule en My Xedule plaatsvinden.

4.1.1 Hoofddoel: Onderwijsplanning

- **Onderwijsadministratie:**

De administratieve ondersteuning van de ontwikkeling van het onderwijs, inclusief het publiceren van een OER en de studiegids.

Bijvoorbeeld: Beheer van onderwijsdocumentatie, faciliteren transparantie voor studenten en medewerkers.

- **Onderwijseenheidsinschrijving:**

Het (impliciet of expliciet) inschrijven van een deelnemer voor een onderwijseenheid.

Bijvoorbeeld: Zowel handmatige als geautomatiseerde inschrijvingsprocessen, waarborgen van accurate deelnemersregistratie.

⁸ [https://hora.surf.nl/index.php/Bedrijfsfunctiemodel_\(detail\)](https://hora.surf.nl/index.php/Bedrijfsfunctiemodel_(detail))

⁹ Het mbo heeft een eigen referentiearchitectuur, de MORA. In bijlage 3 is een vergelijking gemaakt tussen de MORA en de HORA.

- **Toetsinschrijving:**

Het (impliciet of expliciet) inschrijven van een deelnemer voor toetsactiviteiten.
Bijvoorbeeld: Beheer van toetsdeelname, capaciteitsplanning, administratieve ondersteuning.

- **Vraagprognosisering:**

Het maken van een prognose van de hoeveelheid deelnemers en de onderwijsproducten die zij willen afnemen (studentenplanning).
Bijvoorbeeld: Datagedreven besluitvorming, resource management.

- **Lesgroepvorming:**

Het samenstellen van groepen van deelnemers ten behoeve van het gezamenlijk volgen van onderwijsseenheden.
Bijvoorbeeld: Balanceren van groepsgrootte, leerdoelen, beschikbare faciliteiten.

- **Inzet- en middelenplanning:**

Het reserveren van capaciteit van mensen en middelen zodat zij beschikbaar zijn om te voldoen aan de geprognoseerde vraag
Bijvoorbeeld: Personeelsinzet, lokaaltoedeling, apparatuur reservering.

- **Onderwijsactiviteitenplanning:**

Het inplannen van de specifieke activiteiten die in het kader van een onderwijsseenheid noodzakelijk zijn, inclusief het bepalen van de vorm waarin de activiteit zal plaatsvinden (zoals een stage).
Bijvoorbeeld: Flexibiliteit in onderwijsvormen, stage-coördinatie.

4.1.2 Hoofddoel: Roostering

- **Lesroosterconstructie:**

Het koppelen van mensen, middelen en leeractiviteiten op bepaalde momenten in tijd.
Bijvoorbeeld: Minimaliseren conflicten, maximaliseren beschikbaarheid.

- **Roosterwijziging:**

Het aanbrengen van correcties in het rooster zodat deze beter past op de daadwerkelijke beschikbaarheid van mensen en middelen.
Bijvoorbeeld: Real-time aanpassingen, communicatie van wijzigingen.

- **Roosterpublicatie:**

Het beschikbaar stellen van het rooster aan alle relevante doelgroepen.
Bijvoorbeeld: Multikanaal communicatie, gebruiksvriendelijke interfaces.

- **Toetsroosterconstructie:**

Het koppelen van mensen, middelen en toetsactiviteiten op bepaalde momenten in tijd.
Bijvoorbeeld: Concrete aspecten: Capaciteitsbeheer, logistieke ondersteuning.

4.2 Aanvullende verwerkingsdoeleinden

- **Authenticatie/identificatie:**

Zorgdragen voor veilige gebruikerstoegang en verificatie identiteit. Ondersteunen van gedifferentieerde gebruikersrechten.

- **Backup en gegevensherstel:**

Minimaliseren van gegevensverliesrisico's en waarborgen van gegevensintegriteit en continuïteit.

- **Personalisering van dienstverlening:**

Ondersteunen van individuele gebruikersvoorkeuren en efficiënte informatieverstrekking.

- **Fraudepreventie en beveiliging**

Detectie van ongeautoriseerde activiteiten en het beschermen van de systeemintegriteit.

- **Verbetering van de applicaties**

Verbeteren van de applicaties qua prestaties en beschikbaarheid.

- **Marketing en communicatie**

Delen van informatie over (verbetering van) het product

5 Persoonsgegevens

In het eerste lid van artikel 4 van de AVG is de term persoonsgegevens als volgt omschreven:

“persoonsgegevens”: 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 identicator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;”

Xedule sluit met de terminologie in haar Privacy Statement¹⁰ aan bij de term als gedefinieerd in het eerste lid van artikel 4 van de AVG. Gelet op haar gebruikers is deze toelichting dienovereenkomstig aangepast.

“Persoonsgegevens zijn elke vorm van informatie die herleidbaar is naar een uniek, geïdentificeerde of identificeerbare natuurlijke persoon. Voorbeelden hiervan zijn telefoonnummer, e-mailadres, studentnummer, docentcode etc.”

Om de instellingen te helpen een duidelijk en gestructureerd overzicht te verkrijgen van de verschillende soorten persoonsgegevens die worden verwerkt, hanteert SURF de volgende datacategorisatie:

- **Contentdata** Dit omvat kerninformatie waarvoor de applicatie is bedoeld, zoals roosterinformatie (lessen, docenten, lokalen en lestijden), wijzigingen in het rooster en beschikbaarheid van studenten en docenten.
- **Diagnostische data** Dat betreft gegevens die worden verzameld voor het oplossen van problemen, beveiliging en systeemoptimalisatie. Denk aan foutmeldingen en logbestanden (als een gebruiker een foutmelding krijgt).
- **Accountdata** Informatie gerelateerd aan de accounts van de individuele gebruikers en authenticatie. Denk aan inloggegevens en gebruikersrollen.
- **Feedbackdata** Gegevens verkregen uit gebruikersfeedback en -enquêtes.

Opgemerkt dient te worden dat deze overkoepelende DPIA enkel categorieën persoonsgegevens van betrokkenen kan onderscheiden die mogelijk betrokken zijn bij de verwerking. Deze DPIA kan de specifieke risico's van de feitelijke gegevensverwerking per onderwijsinstelling die gebruik maakt of gebruik zal maken van Xedule en My Xedule niet inschatten.

Afhankelijk van de wensen van de onderwijsinstelling, kunnen verschillende bronsystemen worden gekoppeld aan Xedule. Welke persoonsgegevens er uiteindelijk uit deze

¹⁰ Privacy statement Xedule.

bronsystemen worden ingelezen in Xedule hangt af van de rechtmatigheid hiervan en het doel waarvoor Xedule wordt ingezet. Dit wordt nader uitgewerkt in onderdeel B.

Voorafgaand aan iedere wens inzake Xedule en de My Xedule applicaties moeten instellingen een “*Intakeformulier implementatie Xedule*” invullen. Uit het intakeformulier blijkt wat de datawensen zijn en met wie de implementatiemanager Xedule contact kan hebben over de rechtmatigheid van de wensen over onderwijsinstelling. De implementatiemanager van Xedule kan de onderwijsinstelling adviseren op het gebied van de rechtmatigheid van de datawensen. Het gegeven advies is bedoeld als ondersteuning, maar de uiteindelijke keuze en verantwoordelijkheid voor de uitvoering ligt te allen tijde bij de onderwijsinstelling.

Het volledige overzicht van de te verwerken persoonsgegevens is te vinden in *Bijlage 2: persoonsgegevens*. Xedule en My Xedule onderscheiden drie categorieën betrokkenen bij de gegevensverwerkingen die omwille van de omvang en de leesbaarheid van dit document hier al worden benoemd: De eerste twee categorieën zijn de eindgebruikers van My Xedule en de laatste categorie zijn de medewerkers die de roosters opstellen, wijzigen, goedkeuren enzovoorts.

- 1) Studenten onderwijsinstelling (aankomende studenten, studenten, oud student)
- 2) Docenten (docent, instructeur, onderwijsassistent, examinatoren)
- 3) Medewerkers onderwijsinstelling (roosteraar, leidinggevende, team coördinator, staf, systeembeheerder).

Gebleken is dat Xedule de mogelijkheid biedt om alle typen persoonsgegevens uit verschillende bronsystemen¹¹, zoals personeelsinformatiesystemen, in te lezen en hierbij geen onderscheid maakt in de persoonsgegevens. Dat heeft als gevolg dat de mogelijkheid bestaat dat bijzondere persoonsgegevens ook worden ingelezen. Naast het geautomatiseerd inlezen van persoonsgegevens, biedt Xedule de ruimte voor aanvullingen en/of opmerkingen bij het beheren van de beschikbaarheid door middel van handmatige invoer door de roosteraar of de betrokkene zelf. Hierdoor is het ook mogelijk om handmatig (bijzondere) persoonsgegevens in te voeren. Het doel en de rechtmatigheid van de verwerking van deze persoonsgegevens wordt in hoofdstukken 0 en 14 nader uitgewerkt.

¹¹ Voormelde bronsystemen dienen slechts ter illustratie en vallen daarom buiten scope van deze DPIA. Voor alle koppelingen naar Xedule dient separaat door de onderwijsinstelling een inhoudelijke beoordeling plaats te vinden

6 Gegevensverwerkingen

Om de rechtmatigheid van gegevensverwerkingen te kunnen beoordelen, zijn in dit hoofdstuk de verwerkingen in kaart gebracht.

Xedule is de hoofdapplicatie van Xedule en My Xedule is een uitbreiding op de functionaliteit van Xedule. In dit hoofdstuk zijn de verwerkingen beschreven die standaard plaatsvinden in Xedule, en waar van toepassing in My Xedule. Wanneer een verwerking *alleen* op My Xedule van toepassing is wordt deze aangeduid met *[My Xedule]*.

6.1 Roosteren & plannen van onderwijs

De dataset die gebruikt wordt, de werkwijze en processen bij de verwerkingen roosteren & plannen van onderwijs zijn vrijwel gelijk. Om deze reden hebben we deze verwerkingen samengevoegd. We beschrijven hoe de gegevens kunnen worden verzameld, hoe deze kunnen worden gebruikt en hoe deze worden gepubliceerd (gedeeld). Hierdoor ontstaat een duidelijk beeld van de Data Life Cycle binnen deze processen.

Doelbinding:	Roostering, Onderwijsplanning
Categorieën persoonsgegevens:	Contactgegevens, Demografische gegevens Organisatiegegevens, Gezondheidsgegevens, Technische gegevens
Categorieën betrokkenen:	Docent, Medewerker, Student

6.1.1 Geautomatiseerde verzameling

Wanneer er gekozen wordt voor automatische koppelingen worden contactgegevens via API's verzameld. Een API (Application Programming Interface) maakt communicatie tussen verschillende systemen mogelijk. Xedule verzamelt op deze manier data geautomatiseerd via een extract uit bronsystemen, zoals studentinformatiesystemen (SIS) en personeelsinformatiesystemen met behulp van API-koppelingen. Deze gegevens worden vervolgens als kopie van de persoonsgegevens uit deze bronsystemen ingelezen in Xedule.

Xedule biedt ook de mogelijkheid maatwerk API's te bouwen. Bij deze maatwerkoplossingen haalt Xedule gegevens op (GET-aanvragen) uit systemen van de klant. Deze API's worden voornamelijk gebouwd als de klant gebruik maakt van systemen die standaard niet worden ondersteund.

Registratie verlofgegevens: Voor het ondersteunen van Onderwijsplanning (specifiek: Inzet- en Middenplanning) kunnen verlofgegevens van medewerkers in Xedule worden verwerkt, waaronder ook bijzondere persoonsgegevens, zoals zwangerschapsverlof. Deze persoonsgegevens kunnen via de API-koppeling met een HR-systeem worden verzameld (meer in hoofdstuk 7.7 [API's](#)).

6.1.1.1 *Single-Sign-On*

Binnen Xedule en My Xedule wordt Single Sign-On (SSO) ondersteund voor authenticatie van gebruikers. De SSO-oplossing is decentraal ingericht: iedere instelling gebruikt haar eigen SSO-systeem voor medewerkers en studenten. De exacte technische en organisatorische beveiligingsmaatregelen verschillen per instelling, maar de leverancier hanteert gangbare standaarden voor SSO-koppelingen.

6.1.1.2 *[My Xedule] geautomatiseerde verzameling*

My Xedule kan alleen aan Xedule gekoppeld worden voor het geautomatiseerd ophalen van brongegevens. Als front-end voor de eindgebruikers van roosters en inzet- en middelen planning wordt al deze informatie doorgegeven vanuit Xedule.

Voor de doorgifte van informatie, dient de roosteraar deze informatie te publiceren. De roosteraar en functioneel beheerder zijn hier standaard toe bevoegd.

6.1.1.3 *[My Xedule] Locatiegegevens*

Deze functionaliteit is enkel van toepassing wanneer de onderwijsinstelling heeft ingesteld dat gereserveerde ruimtes bevestigd moeten worden. Hij is bedoeld om gereserveerde ruimtes weer beschikbaar te stellen als deze op locatie niet bevestigd is.

Om een reservering op locatie te kunnen bevestigen, verwerkt My Xedule locatiegegevens afkomstig van het gebruikte mobiele apparaat. Dit stelt het systeem in staat te verifiëren of de gereserveerde ruimte daadwerkelijk wordt gebruikt. Om de reservering te bevestigen, moet de gebruiker My Xedule toestemming geven om de locatie van het toestel te gebruiken. Indien deze toestemming nog niet is verleend, zal het besturingssysteem van het apparaat hier automatisch om vragen.

Voorwaarden voor de bevestiging van een faciliteit

- **Locatiebepaling ingeschakeld:** De onderwijsinstelling bepaalt of locatiebepaling in My Xedule is vereist. Als dit is ingeschakeld, wordt de gebruiker bij het openen van de app gevraagd om de locatie te delen.
- **Geen locatie, geen bevestiging:** Als de gebruiker weigert de locatie te delen, is het niet mogelijk om de reservering te bevestigen. Dit komt doordat fysieke nabijheid van de faciliteit een vereiste is voor bevestiging.

Wanneer een reservering binnen de gestelde tijd niet wordt bevestigd, wordt de ruimte automatisch vrijgegeven, zodat anderen deze kunnen gebruiken. Dit voorkomt dat ongebruikte maar gereserveerde ruimtes onnodig bezet blijven.

De locatiegegevens worden eenmalig gebruikt om de bevestiging van de faciliteit te organiseren. Deze worden niet opgeslagen in het systeem.

6.1.2 Handmatige verzameling

6.1.2.1 Export/Import

Wanneer een geautomatiseerde (actieve) koppeling met een bronsysteem niet mogelijk is, kunnen persoonsgegevens handmatig (passief) geïmporteerd worden uit dit bronsysteem, mits dit bronsysteem deze ondersteunt. Hiervoor is het belangrijk dat de benodigde gegevens zijn opgemaakt in een gangbaar formaat (komma gescheiden bestand). De gegevens worden daarna handmatig middels import/export verzameld. Deze import is mogelijk via de interface van Xedule door daartoe geautoriseerde medewerkers. Meer in hoofdstuk 18.10 **Verlies van controle en vertrouwelijkheid door het niet hebben van automatische import/export** **Fout! Verwijzingsbron niet gevonden.**

6.1.2.2 Handmatige invoer

Roosteraars en/of functioneel beheerders kunnen handmatig persoonsgegevens invoeren en bewerken in Xedule. Deze handmatige verwerking vindt plaats via directe invoer in het systeem, waarbij nieuwe gegevens kunnen worden toegevoegd en bestaande gegevens kunnen worden gewijzigd of verrijkt. Denk hierbij aan het handmatig doorvoeren van roosterwijzigingen of toekennen van functies, rollen, groepen en voorkeuren. Persoonsgegevens die geïmporteerd zijn kunnen niet overschreven worden door handmatige invoer. Meer in 18.7 Gemiste kansen en verlies van vertrouwelijkheid door handmatige invoer.

6.1.2.3 Handmatige invoer bijzondere persoonsgegevens

De handmatige invoer van verlofgegevens, afwezigheidsmeldingen en hulpmiddelen verdient een aparte vermelding, daar deze eveneens *input* vormen voor de Inzet- en Middelenplanning van Onderwijsplanning en het Dagroosterbeheer en Toetsroosterconstructie van Roostering.

Verlofgegevens: Voor het ondersteunen van Onderwijsplanning kunnen verlofgegevens van medewerkers in Xedule worden verwerkt, waaronder bijzondere persoonsgegevens, zoals zwangerschapsverlof. Deze persoonsgegevens kunnen zowel door de roosteraar handmatig worden ingevoerd in Xedule of via een geautomatiseerde koppeling met het HR-systeem. Een medewerker kan deze gegevens koppelen aan docenten wanneer aan de medewerker de daarbij horende rol is toegekend.

Acties	Modules	Medewerkers	Kostenplaatsen
Basisdata	Eigenschappen cao	Verlof	Roostervoorwaarden
		Zorgverlof (uren)	Zwangerschapverlof (uren)
		Geboorteverlof (uren)	
		Jaar	Jaar
		0	0
2	Bruir	0	0
3	DijkS	0	0
4	GroeT	300	145
		0	0
6	LindF	0	0
		0	0
8	TESTA	0	0

Figuur 6-1, Invoeren verlofgegevens.

Afhandelen afwezigheidsmeldingen: Een belangrijke functionaliteit van Xedule is dagroosterbeheer. Dagroosterbeheer richt zich op het oplossen van last-minute roosterconflicten. Tijdens dit proces kunnen de roosteraars de reden van het roosterconflict registreren, denk bijvoorbeeld aan afwezigheid van docent door ziekte. Deze gegevens kunnen bijzondere persoonsgegevens bevatten, daar ziekmeldingen kunnen worden geregistreerd. Roosteraars en/of beheerders kunnen deze wijzigingen (conflicten) labelen via een picklist. Instellingen kunnen zelf bepalen hoe ze de labeling inrichten. Voor de roosteraar zijn de 'wijzigingsredenen' van belang, aangezien deze gebruikt worden om roosterwijzigingen achteraf te analyseren, evalueren en waarderen. Dit stelt de roosteraar in staat om toekomstige roosterwijzigingen effectiever af te handelen. Dit is voor veel instellingen essentieel omdat roostermutaties een groot probleem vormen voor de onderwijscontinuïteit.

MyX	Configuratie	Acties	Modules	Medewerkers
Code	Wijzigingsreden	Aantal onopgeloste co	Vanaf	Tot en met
1	Scholing	0	8-1-2025 00:00	9-1-2025 23:59
2	bruir_ziek	5	19-8-2024 00:00	30-12-2024 23:59

Figuur 6-2, registreren reden roosterwijziging via een picklist.

Het is de keuze en daarmee verantwoordelijkheid van de onderwijsinstelling om de reden van afwezigheid te registreren in Xedule en My Xedule. Meer in hoofdstuk 18.3 **Verlies van vertrouwelijkheid en sociaal nadeel door te brede definiëring afwezigheids- en hulpmiddelencategorieën.**

Registratie hulpmiddelen: Ter ondersteuning van toetsroosterconstructie worden hulpmiddelen voor studenten met extra afspraken rond voorzieningen bij toetsafname handmatig ingevoerd door roosteraars en/of andere medewerkers die daarvoor zijn aangesteld en gemachtigd. Deze hulpmiddelen worden toegekend vanuit een picklist¹² die door onderwijsinstelling wordt beheerd. Deze gegevens zeggen iets over de fysieke of mentale gezondheid van de betrokkene en worden daarom gekwalificeerd als bijzondere persoonsgegevens. Meer in hoofdstuk 18.3 **Verlies van vertrouwelijkheid en sociaal nadeel door te brede definiëring afwezigheids- en hulpmiddelencategorieën.**

6.1.2.4 Vrije velden: opmerking

Xedule heeft vrije velden beschikbaar zonder een gespecificeerd doel (zie Figuur 6-3). Hiermee is het mogelijk om een opmerking aan een gebruiker te hangen, het is de onderwijsinstelling vrij om hier invulling aan te geven.

	Basisdata	Eigenschappen cao	Verlof	Roostervoorwaarden	Medewerkertypes	Teams	Contracttype	Voorkeursfaciliteiten	Expertises	
	Personeelsnumr	Voornaam	Achternaam	E-mail	Gebruikersnaam	Opmerking				Bes
										He
2	Bruir	Rick	de Bruin	r.de.bruin@surf.nl	XEDULE\surf_bruir	Test opmerking Bruir				75
3	DijkS	Sanne	van Dijk	s.v.dijk@surf.nl	XEDULE\surf_dijks	Test opmerking DijkS				75
4	GroeT	Thijs	Groenewoud	t.groenewoud@surf.nl	XEDULE\surf_groet	Test opmerking GroeT				75
										75
										75
										75
										+

Figuur 6-3, Vrij veld bij een gebruiker.

Deze zijn voor de daartoe gemachtigde gebruikers zichtbaar. Xedule heeft in het openingsscherm van de gebruiker een disclaimer opgenomen om de kaders en het doel van deze vrije invulvelden te duiden (zie Figuur 6-4). De link in de disclaimer leidde in de testomgeving naar een foutmelding.

¹² Een picklist is een lijst met vooraf gedefinieerde opties waaruit een gebruiker kan kiezen.



Figuur 6-4, disclaimer rond vrije invulvelden.

Volgens Xedule leidt de link in de omgeving van instellingen naar de privacyverklaring (zie figuur 6-5). Dit heeft SURF niet kunnen verifiëren. Meer hierover in hoofdstuk 18.6 **Verlies van controle en vertrouwelijkheid door overige vrije velden.**

VISMA | advitiae Zoeken

Deze pagina: Juridisch \ Privacyverklaring

Privacyverklaring van Xedule (Visma Advitiae)

Inleiding

Als je de applicaties Xedule of My Xedule (MyX) gebruikt en diensten afneemt bij Xedule (Visma Advitiae), verzamelt Xedule (Visma Advitiae) persoonsgegevens van jou. Bij het bezoeken van de website(s) van Xedule (Visma Advitiae) worden ook persoonsgegevens verzameld door Xedule (Visma Advitiae).

Persoonsgegevens zijn elke vorm van informatie die herleidbaar is naar een uniek, geïdentificeerde of identificeerbare natuurlijke persoon. Voorbeelden hiervan zijn telefoonnummer, e-mailadres, studentnummer, docentcode enzovoort.

Dit Privacy Statement helpt je te begrijpen welke persoonsgegevens wij van je verzamelen, waarom wij de persoonsgegevens verzamelen en hoe Xedule (Visma Advitiae) met jouw persoonsgegevens omgaat.

Aanvulling met betrekking tot het gebruik van vrije velden

Afhankelijk van de inrichting van Xedule en de toegekende rollen van gebruikers binnen Xedule wordt autorisatie gebruikt om met een minimale set aan (persoons)gegevens de werkzaamheden uit te voeren. Door autorisaties correct toe te passen wordt voldaan aan het beginsel van de AVG met een zo klein mogelijke dataset het werk uit te voeren.

Daarnaast beschikt Xedule over andere velden waarin vrije teksten bewaard kunnen worden. Dit zijn velden met aanvullende opmerkingen of notities over personen en die een gebruiker (een roostermaker of planner) op eigen initiatief invult. Doordat deze velden vrij ingevuld kunnen worden bestaat de kans dat het veld informatie bevat die niet aan de eisen van de AVG en de Verwerkersovereenkomst voldoet.

Dit valt onder de verantwoordelijkheid van de Verwerkingsverantwoordelijke, dit is de onderwijsinstelling. Het advies over het gebruik van de vrij in te vullen velden is dan ook om géén persoonsgegevens te noteren in velden die bedoeld zijn voor opmerkingen en notities. Ook mogen geen bijzondere persoonsgegevens hier ingevuld worden.

Voor verdere instructies of hulp bij het gebruik van Xedule wordt verwezen naar de functioneel beheerder van Xedule.

Persoonsgegevens waarvoor Xedule (Visma Advitiae) Verwerker is

Voor alle persoonsgegevens die opgenomen zijn in de applicaties die Xedule (Visma Advitiae) aanbiedt en die door Xedule (Visma Advitiae) worden verwerkt, is jouw school of onderwijsinstelling de *Verwerkingsverantwoordelijke*. Dit houdt in dat Xedule (Visma Advitiae) jouw persoonsgegevens in opdracht en conform instructies van jouw onderwijsinstelling verwerkt. Xedule (Visma Advitiae) is daarmee de *Verwerker*.

Figuur 6-5, Tekst over vrije invulvelden.

6.1.2.5 |My Xedule| Beschikbaarheid

Als front-end voor docenten is het mogelijk dat docenten via My Xedule hun beschikbaarheid (roostervoorwaarden) doorgeven aan Xedule. My Xedule fungeert hierin als interface voor de docenten. Bij het doorgeven van beschikbaarheid kan een motivatie (comment) mee worden gestuurd via een vrij veld. Het is zeer aannemelijk dat er gevoelige of zelfs bijzondere persoonsgegevens in deze velden worden verwerkt. Deze motivatie wordt gedeeld met de leidinggevende welke de beschikbaarheid fiatteert. Als deze is goedgekeurd wordt deze inclusief motivatie doorgezet naar de roosteraar. Meer in hoofdstuk 18.5 **Verlies van vertrouwelijkheid door doorgeven beschikbaarheidsredenen aan roosteraars.**

Je beschikbaarheid voor 2024-2025.

☒ WEEKSTRUCTUUR
 ☒ 2 OPMERKINGEN
 ☐ 3 BEVESTIGEN

Heb je een opmerking over je beschikbaarheid op een specifiek tijdstip? Klik dan in het betreffende vak en zet je opmerking erbij.
 Opmerkingen zijn zichtbaar voor de teamleider en roostermaker.

	MAANDAG	DINSDAG	WOENSDAG	DONDERDAG	VRIJDAG
08:30 - 13:00	☒	☐	☒	☒	☒
Opmerking over de beschikbaarheid op maandag 08:30 - 13:00					
13:00 - 17:30	☒	☐	☒	☒	☒
17:30 - 20:00	☒	☐	☒	☒	☒

[TERUG](#)
[VERDER](#)

Figuur 6-6, vrij invulveld bij doorgeven beschikbaarheid.

6.1.2.6 |My Xedule| Inschrijven

Als front-end voor studenten is het mogelijk dat studenten zich via My Xedule inschrijven voor daartoe ingerichte vakken en/of faciliteiten. My Xedule fungeert hierin als interface voor de studenten. Studenten kunnen via een vrij veld een motivatie meegeven bij het inschrijven voor een vak/faciliteit (meer in hoofdstuk 18.6 **Verlies van controle en vertrouwelijkheid door overige vrije velden**).

Wo 18 sep 09:00-10:00 ✕

Sluit over één dag.

VAK
Bijles praktijk

GROEP
Klas 01, Klas 02, Klas 03, Klas 04

DOCENT


FACILITEIT
Praktijk03

OMSCHRIJVING
Bijles praktijk

MOTIVATIE OF OPMERKING
Motivatatie of opmerking

Figuur 6-7, voorbeeld inschrijving

6.1.3 Opslag

Alle verwerkte persoonsgegevens worden opgeslagen binnen de EER, specifiek in Nederland, bij Interconnect. De gegevens in rust (*data at rest*) worden versleuteld opgeslagen. Hoewel de database zelf niet versleuteld is, worden back-ups, die daadwerkelijk als *data at rest* worden beschouwd, wel versleuteld met AES-128.

Op het moment van schrijven heeft Xedule mondeling aangegeven bezig te zijn met het onderzoek of het versleutelen van de gehele database mogelijk is, er is op dit moment geen zicht op wanneer dit gerealiseerd is en hoe.

Daarnaast staat de database op een storage-unit met redundante schijven, waarop volledige schijfversleuteling (*Full Disk Encryption*, FDE) is geactiveerd. Deze encryptie voldoet aan de AES-256 standaard en de FIPS 140-2 certificering.

Zie hoofdstuk 7.6 *Encryptie* voor meer informatie over hoe en wanneer encryptie wordt toegepast in deze verwerking.

Zie hoofdstuk 8.8 *Derden* voor meer informatie over Interconnect, de hosting partij waar deze verwerking plaatsvindt.

6.1.4 Datamanagement

Functioneel beheerders van instellingen zorgen binnen Xedule voor een inrichting waar accountdata en contentdata geordend, gestructureerd en verrijkt kunnen worden met organisatiegegevens. Zo worden er door roostermakers onder andere lesroosters opgesteld en klasgroepen ingericht, dit wordt gedaan door ruimtes/faciliteiten, datum en tijd en personen aan elkaar te koppelen. Roosteraars en functioneel beheerders kunnen, afhankelijk van hun autorisatie, via Xedule de al ingelezen contentdata wijzigen en/of bijwerken. Zoals eerder is benoemd, is de accountdata in Xedule een kopie van de persoonsgegevens (stamgegevens) uit het bronsysteem wat gekoppeld is aan Xedule. De stamgegevens kunnen in Xedule niet gemuteerd worden. Mochten er mutaties in de stamgegevens nodig zijn (bijvoorbeeld in geval van uitoefening van recht tot rectificatie), dan kunnen deze mutaties enkel plaatsvinden binnen de bronsystemen. Vervolgens worden de mutaties, doordat de persoonsgegevens opnieuw worden ingelezen, automatisch doorgevoerd in Xedule.

Een terugkomend element is het uitgebreide gebruik van tabellen in de interface. Vrijwel alle gegevens worden weergegeven door middel van deze tabellen, die in de basis een zeer toegankelijke manier om te kopiëren bieden. Dit maakt het kopiëren en exporteren van gegevens eenvoudig, wat kan leiden tot schaduwadministratie. Meer in hoofdstuk 18.11

Verlies van controle en vertrouwelijkheid door tabellen.

Eigenschappen cao		Verlof	Roostervoorwaarden	Medewerkertypes	Teams	Contracttype	Voorkeursfaciliteiten	Expertises	Informatie	MyX
								Beschikbaar		
								Herhaal 1 week p		Filter Alles
Voornaam	Achternaam	E-mail	Gebruikersnaam	Opmerking	Ma	Di				
Rick	de Bruin	r.de.bruin@surf.nl	XEDULE\surf_bruir	Test opmerking BruiR	75	75				
Sanne	van Dijk	s.v.dijk@surf.nl	XEDULE\surf_dijk	Test opmerking DijkS	75	75				
Thijs	Groenewoud	t.groenewoud@surf.nl	XEDULE\surf_	Kopieer alle data naar klembord	75	75				
Kolommen selecteren >					✓ Basisdata	75				
					Eigenschappen cao	75				
					Verlof	75				
					Roostervoorwaarden	75				
					Medewerkertypes	+				
					Teams					
					Contracttype					
					Voorkeursfaciliteiten					
					Expertises					
					Informatie					
					MyX					
					Aanpassen...					

Figuur 6-8, kopiëren uit interface Xedule.

6.1.5 Publiceren

Het delen van informatie kan intern plaatsvinden of extern met dienstverleners, klanten enzovoorts. Alleen die gegevens die de ontvanger nodig heeft, moeten worden gedeeld. Waar mogelijk moeten gegevens worden geanonimiseerd, geminimaliseerd of geaggregeerd voordat ze worden gedeeld.

6.1.5.1 Publiceren via My Xedule

De persoonsgegevens worden getoond in My Xedule. Studenten en docenten hebben hiermee toegang en inzage tot hun eigen roosterinformatie en faciliteitsreserveringen. Sommige medewerkers (docenten) kunnen -wanneer de autorisatie daarop is ingericht- ook roosters van andere gebruikers (studenten en/of docenten) inzien. Dit is een onderwijsinstellingsafhankelijke instelling en naar eigen inzicht in te richten.

6.1.5.2 Delen via API's

Om gegevens met andere applicaties te delen kan er, op het moment van schrijven van deze DPIA, gebruik gemaakt worden van drie verschillende API's. Via API's kunnen geautomatiseerd gegevens tussen twee systemen worden uitgewisseld.

Xedule REST API: Alle gegevens die een eindgebruiker met de hoogste rechten in de Graphical User Interface GUI van Xedule kan inzien, zoals een functioneel beheerder, vallen onder de scope van wat er is op te halen met deze API. Andere gegevens kunnen dus niet opgehaald worden door deze API.

Xedule Management SOAP API: Dit is een verouderde (deprecated) API die nog door enkele instellingen wordt gebruikt. Hieraan worden geen nieuwe functies toegevoegd.

Xedule Connect: Zoals de vorige twee API's, dient Connect als een manier om gegevens uit Xedule op te halen. Het grote verschil met de voornoemde API's is dat authenticatie naar de in Connect aangemaakte API's verloopt via een verbeterd protocol waarbij de beveiliging zonder tussenkomst van Xedule ingeregeld kan worden. Meer in *hoofdstuk 7.7 API's*.

6.1.5.3 |My Xedule| API's

Net zoals Xedule, biedt My Xedule ook enkele API's aan om gegevens te delen met andere applicaties. Meer in *hoofdstuk 7.7 API's*.

6.1.5.4 |My Xedule| Synchronisatie

My Xedule biedt studenten en docenten de mogelijkheid om hun roosterinformatie te integreren met diverse digitale agenda-diensten door middel van (open) agenda-standaarden (Graph API, Export ICS en Rooster feed). Deze functionaliteit stelt eindgebruikers in staat om hun roosters te synchroniseren met platforms zoals Outlook, Apple Calendar, Google Calendar en andere externe agenda-applicaties. Het is belangrijk om te benadrukken dat deze integratie volledig optioneel is en alleen wordt geactiveerd door de eindgebruiker zelf. De gegevensuitwisseling verloopt hierbij uitsluitend in één richting: van My Xedule naar de gekozen agenda-applicatie.

Graph API: Een geautomatiseerde koppeling met andere agenda applicaties. Meer in *hoofdstuk 7.7 API's*.

Export ICS: Dit is een gedownloade kopie van een rooster die ingelezen kan worden in agenda-applicaties. Dit bestand is daarmee in beheer van de betrokkene en wordt niet meer beheerd door Xedule, het bestand heeft ook geen koppeling meer met Xedule/My Xedule.

Rooster feed: Dit is een digitaal abonnement op een rooster waarmee het rooster tot 10 weken vooruit binnengehaald kan worden door de betrokkenen en betreft alleen groepen (klassen) gekoppeld aan faciliteiten (zoals lokalen en andere lesruimten). Autorisatie vindt plaats door My Xedule, heeft de betrokkene toegang tot dit rooster in My Xedule mag de betrokkene de koppeling maken.

6.1.6 Verwijdering van gegevens

Bewaartermijnen dienen door instellingen te worden vastgesteld en nageleefd. In Xedule is er geen ingebouwde functionaliteit beschikbaar voor het beheren van bewaartermijnen. Het systeem voorziet niet in automatische verwijdering van gegevens en gegevens kunnen niet als 'te verwijderen' worden gemarkeerd. Daarnaast is er geen aparte functionaliteit is om bijzondere en/of gevoelige gegevens die Xedule verwerkt apart te selecteren, groeperen en/of te labelen (ter verwijdering).

Het is momenteel voor een onderwijsinstelling op drie manier mogelijk om persoonsgegevens te verwijderen.

- 1 Het verwijderen van een ORE (Organisatie Rooster Eenheid). Een ORE bevat doorgaans roostergegevens voor één academisch jaar, samen met gegevens van een specifieke opleiding, instituut en/of gebouw. Het is echter niet gedocumenteerd welke impact het verwijderen van een ORE heeft op gerelateerde data in het systeem.
- 2 Het handmatig verwijderen van gegevens uit de diverse aanwezige tabellen. Deze aanpak vereist een zorgvuldige uitvoering om de data-integriteit te waarborgen.
- 3 Het indienen van een verwijderverzoek bij Xedule, al is er geen gedocumenteerde procedure beschikbaar voor het indienen van dergelijke verzoeken.

Xedule en My Xedule bieden niet de mogelijkheid om persoonsgegevens na het verstrijken van de bewaartermijn automatisch te verwijderen. Vooropgesteld wordt dat instellingen als verwerkingsverantwoordelijke zelf zorg dienen te dragen voor het bewaken van de bewaartermijnen en dat deze gegevens dienovereenkomstig worden verwijderd. Het gebrek aan automatische verwijderingsfunctionaliteit betekent echter wel dat instellingen de bewaartermijnen zelf handmatig dienen te monitoren en handhaven. Meer in hoofdstuk 18.8 Verlies van controle en vertrouwelijkheid door niet automatisch te configureren bewaartermijnen.

6.2 Beheer

Beheersprocessen zijn de processen die Functioneel Applicatie Beheer van de Onderwijsinstelling uitvoert om te zorgen dat de inrichting van de Xedule/My Xedule conform implementatie plan wordt ingeregeld.

Doelbinding:	Roostering, Onderwijsplanning, Authenticatie/identificatie
Categorieën persoonsgegevens:	Contactgegevens, Organisatiegegevens, Technische gegevens
Categorieën betrokkenen:	Docent, Medewerker, Student

6.2.1 Identiteits- en toegangsbeheer

In dit kader worden persoonsgegevens verwerkt om toegang te beheren en systemen te beveiligen. Identiteits- en toegangsbeheer zorgt ervoor dat alleen geautoriseerde personen toegang hebben tot de data. Binnen Xedule kunnen Rollen worden aangemaakt. Deze zijn te koppelen aan acties. Acties zijn de handelingen die Xedule-gebruikers kunnen uitoefenen, variërend van inzien van gegevens tot het aanpassen of verrijken van gegevens. Wanneer de handelingen die gebruikers kunnen doen zijn gebaseerd op de rollen die ze hebben, heet dit *role-based access* (RBAC).

Standaard zijn er rollen beschikbaar die Xedule heeft ingericht op basis van ‘best-practices’. Maar rollen zijn ook door de beheerders aan te maken, te wijzigen en te specificeren.

De standaard rollen zijn: opleidingsmanager, functioneel beheerder, onderwijsontwikkelaar, planner en roosteraar¹³.

Wanneer een actie aan een gebruikersrol toegekend wordt, zal een rechtenniveau gedefinieerd moeten worden voor die actie. Xedule maakt onderscheid tussen beheer-, schrijf- en leesrechten¹⁴:

- Leesrechten: Een gebruiker kan data inzien afhankelijk van de teamautorisaties die zijn toegekend aan de data en de teamrechten die de gebruiker heeft om data van bepaalde teams te mogen zien.
- Schrijfrechten: Een gebruiker kan data aanmaken, verwijderen, aanpassen en lezen, afhankelijk van teamautorisaties die zijn toegekend aan de data en de teamrechten die de gebruiker heeft om data van bepaalde teams te mogen zien en bewerken.
- Beheerrechten: Een gebruiker kan data lezen, aanmaken, verwijderen en aanpassen, onafhankelijk van de teamautorisaties die zijn toegekend aan de data.

Autorisaties voor (bijzondere) persoonsgegevens kunnen op veldniveau worden ingericht, zodat er gedetailleerde rollen kunnen worden aangemaakt. Dit autorisatiemodel is opgezet met het oog op de uiteenlopende wensen en eisen van instellingen. Instellingen kunnen per veld bepalen of deze (on)zichtbaar en/of (on)bewerkbaar is voor specifieke gebruikers of rollen. Hierdoor is het mogelijk om de toegang tot gegevens te regelen en aan te passen aan de eigen beleidskeuzes.

Bij oplevering van de applicaties is er standaard geen toegang tot persoonsgegevens. De eerste toegang wordt verstrekt aan de Functioneel Beheerder van de onderwijsinstelling door de adviseur of consultant van Xedule. Deze adviseur/consultant heeft gedurende het implementatieproject tijdelijk volledige toegang om de inrichting te begeleiden. Na afronding van het project wordt deze toegang ingetrokken en ligt het beheer volledig bij de onderwijsinstelling.

Het is niet mogelijk om gebruikers via een extern identiteits- en toegangsbeheersysteem geautomatiseerd autorisaties toe te kennen. Gebruikers dienen handmatig aan een van de groepen gekoppeld te worden binnen Xedule (meer in hoofdstuk 18.12 [Verlies van vertrouwelijkheid door handmatige RBAC](#)).

¹³ Xedule Help \ Beheer \ Autorisatie \ Gebruikersgroepen.

¹⁴ Xedule Help \ Beheer \ Autorisatie \ Acties.

6.2.2 Configuratie

Functioneel beheerders kunnen binnen Xedule diverse systeeminstellingen aanpassen. Veel van deze instellingen hebben directe invloed op de autorisatiestructuur van Xedule en afzonderlijk van My Xedule. Voor het begrijpen van de impact van deze instellingswijzigingen is raadplegen van de handleiding die beschikbaar is in de applicatie zelf noodzakelijk (meer in hoofdstuk 18.13 [Verlies van vertrouwelijkheid door onduidelijke configuratiewijzigingen](#)).

Rechten

ⓘ Na opslaan, worden wijzigingen binnen enkele minuten zichtbaar in MyX.

☐ In myx bekende gebruikers hebben alleen autorisatie tot roosters uit hun eigen organisatorische eenheden

Docent mag op het rooster de beschikbaarheid zien van ...

☒ Docenten ☒ Lokalen

Student mag op het rooster de beschikbaarheid zien van ...

☒ Docenten ☒ Lokalen

Docent mag roosters zien van ...

☒ Docenten ☒ Groepen ☒ Lokalen ☒ Middelen ☒ Studenten ☐

Student mag roosters zien van ...

☒ Docenten ☐ Groepen ☒ Lokalen ☐ Studenten

☒ Inzien plannen van inzet voor teams toestaan voor medewerkers

☒ Toon medewerkers en groepen bij gemeenschappelijke vakken en taken in plan van inzet

☐ Docent mag lessen online beschikbaar maken

Redirect voor niet geautoriseerde gebruikers

☐ Toon RE informatie op activiteiten in het rooster

☐ Online lessen openbaar toegankelijk maken voor myx gebruikers met toegang tot roosters

Toets deelnemer metadata web hook

Metadata

Reset

Opslaan

Figuur 6-9, screenshot systeeminstellingenscherf van My Xedule in Xedule.

6.3 Logging

Om een overzicht van de logpraktijken van Xedule binnen Xedule en My Xedule te krijgen is het logbeleid bestudeerd en zijn er inzageverzoeken gedaan (meer over inzageverzoeken in hoofdstuk 6.4 Inzageverzoeken).

Het logbeleid van Xedule is na opleveren onderdeel A van deze DPIA gedeeld met SURF, onderdeel A is op basis van deze informatie herzien.

Dit logbeleid¹⁵ kan geen duidelijkheid geven in de volgende onderwerpen:

1. Wie is er wanneer geautoriseerd om de logs in te zien?
 - Welke procedures liggen hieronder ten grondslag?
2. Welke persoonsgegevens worden er verwerkt per type logging?
 - Heeft Xedule zelf een proportionaliteitsafweging gemaakt?
3. Welke besluiten heeft Xedule genomen om de scope van de logging te bepalen?
4. Welke besluiten heeft Xedule genomen bij het inrichten van party log systemen?

¹⁵ Xedule Logging | 2025 Logging.pdf.

Xedule hanteert zelf categorisering van drie soorten logging:

1. Applicatielogging
2. Systeemlogging
3. Overige logging

Zie ook 18.2 *Verlies van controle door gebrek aan transparantie logging, pNPS en marketing.*

Doelbinding:	Fraudepreventie, Authenticatie/identificatie, Klantondersteuning, Fraudepreventie en beveiliging, Verbeteren van de applicaties
Categorieën persoonsgegevens:	Contactgegevens, Technische gegevens
Categorieën betrokkenen:	Docent, Medewerker, Student

6.3.1 Applicatielogging

Applicatielogging is logging dat binnen de applicatie plaatsvindt en die zich onderscheidt van systeemlogging omdat deze toegankelijk is voor de (functioneel applicatie) beheerders van betreffende onderwijsinstelling. Deze logging wordt als 'read only' opgeslagen en is daarmee op de originele locatie niet te wijzigen. Deze applicatielogging is gebaseerd op de onderliggende applicatielogging (zie **Fout! Verwijzingsbron niet gevonden.**).

Vastgelegde gegevens	Doel	Omschrijving
Gebruikersnaam van gebruiker	Authenticatie/identificatie	Identificatie van gebruiker
Aanmeldgegevens zoals datum en tijd	Authenticatie/identificatie	Herleidbaarheid van moment van aanmelden
Foutieve aanmeldingen	Authenticatie/identificatie	Zichtbaarheid van foutieve aanmeldingen
Acties (verwerkingen) door gebruiker zoals wijzigingen	Fraudepreventie	Herleidbaarheid van wijzigingen een 'audit trail'.
Gebruikte besturingssystemen	Klantondersteuning	Info die gebruikt wordt bij klantondersteuning.
Gebruikte browsers	Klantondersteuning	Info die gebruikt wordt bij klantondersteuning.

Tabel 6-1

De bewaartermijn op applicatielogging in de productie omgeving is maximaal 6 maanden.

De bewaartermijn op applicatielogging in de acceptatie omgeving is maximaal 3 maanden, tenzij onderwijsinstelling afziet van (de automatische Deze bewaartermijn gaat in op moment van verzamelen.) verversing van deze omgeving.

6.3.2 Systeemlogging

Logging van de infrastructurele onderdelen van de SaaS-oplossing. De combinatie van log informatie maakt deel uit van de mogelijkheden om te voldoen aan verzoeken van betrokkenen, analyses rondom informatiebeveiliging/datalekken en foutanalyses.

6.3.2.1 Internet Information Server (IIS)

Logging van toegang tot de Internet Information Server.

Vastgelegde gegevens	Doel	Omschrijving
IP-adressen waarvandaan toegang gevraagd wordt	Fraudepreventie en beveiliging	Mogelijkheid om toegang op het IP-adres te blokkeren. Beveiligingsmaatregel om toegang te beperken. Analyse bij troubleshooten.
Datum en tijd	Fraudepreventie en beveiliging	Het terug kunnen vinden van aanmeldingspogingen van gebruikers.
Gebruikers My Xedule	Fraudepreventie en beveiliging	Synchronisaties tussen My Xedule en Xedule worden gelogd.
URL-informatie	Fraudepreventie en beveiliging	Toegangscontrole op URL-niveau.

Tabel 6-2, overzicht Internet Information Server logging.

De bewaartermijn op applicatielogging is maximaal 6 maanden.

6.3.2.2 Front-end en back-end logging

Binnenkomst op het platform en de verbinding naar onder andere de databaseserver wordt vastgelegd.

Vastgelegde gegevens	Doel	Omschrijving
Sessie identificatie	Fraudepreventie en beveiliging	Gebruikers moeten met een correcte sessie ID doorgezet worden naar de verwerkende kant van het platform, de back-end.

Datum en tijd	Fraudepreventie en beveiliging	Timestamp voor analyse doeleinden en geldigheid van de sessies
Acties van de gebruiker (gedetailleerd)	Fraudepreventie en beveiliging, Verbetering van de applicatie	Elke actie van een gebruiker wordt gelogd teneinde inzicht te krijgen bij misbruik, datalekken, fouten van de applicatie, foutief gebruik van de applicatie en verbeteren van de applicatie.
Systeemgegevens van gebruiker zoals ip-adres, besturingssysteem en browsergegevens	Fraudepreventie en beveiliging	Informatie wordt gebruikt voor onderzoeksactiviteiten als fouten in de applicatie gemeld worden.

Tabel 6-3, overzicht frontend backend logging.

De bewaartermijn op front-end en back-end logging is maximaal 6 maanden.

6.3.2.3 Overige applicatielogging

Overige logging processen rondom verwerkingen binnen Xedule & My Xedule.

Vastgelegde gegevens	Systeem	Doel	Omschrijving	Bewaartermijn
Externe ip-adressen en dataverkeer.	Firewall logs	Fraudepreventie en beveiliging	Bescherming tegen ddos, ongewenste toegang en analyse mogelijkheden om toegang te beperken.	Maximaal 7 dagen
Geaggregeerde informatie ten behoeve van monitoring op hard- en software prestaties. (zie	Azure Insights	Fraudepreventie en beveiliging, Verbetering van de applicatie	Verbeteren van het platform qua prestaties en beschikbaarheid. My Xedule legt enkel de	Maximaal 90 dagen

*Microsoft Azure Application Insights)			namen van gebruikers vast en is nodig voor input voor plannen/roosteren	
--	--	--	---	--

Tabel 6-4

***Microsoft Azure Application Insights:** Het verwerken van technische gegevens via Azure Insights stelt Xedule in staat om de stabiliteit en functionaliteit van de applicaties te monitoren, technische problemen vroegtijdig te identificeren en de gebruikerservaring te verbeteren. Dit doet Xedule onder andere door opeenstapelingen van onsuccesvolle activiteiten te signaleren en op onderwijsinstellingsniveau automatisch te melden bij de ontwikkelaars van Xedule.

In het logbeleid worden de in dit proces verwerkte gegevens niet verder gespecificeerd dan “Geaggregeerde informatie ten behoeve van monitoring op hard- en software prestaties.”

Vanuit de technische analyse (zie bijlage 20.1 **Onderschepte data** een voorbeeld van onderschepte data) is gebleken dat er in de basis technische gegevens worden doorgegeven aan Microsoft Azure Application Insights. Onduidelijk was hierbij of het IP-adres van de betrokkene ook wordt verwerkt.

Xedule heeft mondeling aangegeven dat zij zelf de username van de gebruiker doorgeven aan Microsoft Azure Application Insights, daar waar in de basis Microsoft Azure Application Insights de gebruiker en de sessie heeft gepseudonimiseerd.

Microsoft, waarvan het hoofdkantoor zich in de Verenigde Staten bevindt, is leverancier van Azure Insights. Microsoft is hiermee verwerker voor Xedule. Niet bekend is of en welke afspraken hieromtrent zijn gemaakt tussen Xedule en Microsoft. Meer in hoofdstuk 18.2 **Verlies van controle door gebrek aan transparantie logging, pNPS en marketing.**

6.4 Inzageverzoeken

In het kader van ons onderzoek heeft SURF inzageverzoeken (DSARs) ingediend bij Xedule. Dit gebeurde naar aanleiding van de verschillende scenario's (zie 20.2 **Test**) die wij hebben uitgewerkt in Xedule en My Xedule. Tijdens deze scenario's waren diverse actoren betrokken, waaronder twee docenten, twee studenten, een roostermaker en een leidinggevende. Vanuit praktische overwegingen waren dit fictieve gebruikers. Om de kans op een volledige en correcte afhandeling te vergroten, hebben wij bij ieder verzoek verschillende identificatoren (zie 20.3 **Voorbeeld inzageverzoek**) meegezonden. Deze identificatoren bevatten ook de gepseudonimiseerde id's die aan de betrokkene waren toegewezen ten behoeve van logging.

Voor elk van deze betrokkenen hebben wij een inzageverzoek (DSAR) ingediend bij Xedule. Deze inzageverzoeken (zes stuks) worden gedaan om:

- Inzicht te geven in de verwerkte persoonsgegevens;
- Verduidelijking te geven van redenen achter de verwerkingen;
- En meer informatie te verkrijgen over verwerkingen die onder verantwoordelijkheid van Xedule plaatsvinden.

Na het doen van onze verzoeken, hebben wij slechts op één inzageverzoek, (die van de leidinggevende), een reactie ontvangen van Xedule. Ondanks de goede intenties van Xedule volgde de officiële reactie pas na het verstrijken van de wettelijke termijn van 30 dagen. Daarnaast is er geconcludeerd dat de terugkoppeling op het inzage verzoek onvolledig was.

Uitkomsten van de DSAR uitvraag:

Verstreckte gegevens betrokkene “leidinggevende”:

- Contactgegevens
- Organisatiegegevens

Uit de DSAR ontbrekende gegevens:

Technische gegevens; van de loggegevens werden er uitsluitend logs van inlogpogingen verstrekt, terwijl de resterende loggegevens (zie 6.3.2.2 Front-end en back-end logging en 6.3.2.3 Overige applicatielogging) ontbraken.

Doordat we alleen een reactie hebben gehad op de leidinggevende hebben we geen bijzondere persoonsgegevens verstrekt gekregen, deze waren verwerkt onder een andere betrokkene.

Door het ontbreken van de volledige loginformatie in de ontvangen DSAR is het onmogelijk om een volledig beeld te vormen van de logging en daarmee de verwerking van persoonsgegevens binnen Xedule en My Xedule (*Meer zie hoofdstuk 18.9 Niet uit kunnen oefenen van AVG-rechten door incomplete inzageverzoeken*)

7 Technieken en methoden van de gegevensverwerkingen

7.1 Software-as-a-Service

Xedule en My Xedule zijn Software-as-a-Service (SaaS) oplossing waarbij de applicatie en bijbehorende data worden beheerd door de leverancier. Dit betekent dat beide applicaties via webbrowsers toegankelijk zijn voor geautoriseerde gebruikers, zonder dat er lokale installatie van software nodig is. Updates en onderhoud worden centraal uitgevoerd door de leverancier. De toegang tot de applicatie verloopt via versleutelde verbindingen (HTTPS), waarbij authenticatie van gebruikers plaatsvindt voordat toegang wordt verleend tot de applicatie.

7.2 Geautomatiseerde besluitvorming¹⁶

De applicatie maakt van een systeem dat automatisch voorstellen doet voor (de meest optimale) roosterindelingen op basis van beschikbaarheid, locatiegegevens en roostervoorwaarden. Dit systeem is niet lerend en genereert met dezelfde input en voorwaarden altijd dezelfde uitkomst. Vanuit het systeem wordt het rooster nooit automatisch gepubliceerd, deze gegenereerde roosters worden in concept aan de roosteraar opgeleverd. De roosteraar neemt dan de uiteindelijke beslissing over het rooster en de applicatie dient dan slechts als hulpmiddel.

7.3 Backup¹⁷

Om de continuïteit van de dienstverlening te waarborgen hanteert Xedule een gelaagd back-up-systeem. Dit bestaat uit de volgende componenten:

- Data staat op twee fysieke locaties¹⁸, Eindhoven en Den Bosch;
- Xedule kan bij langere ‘downtime’ van een datacenter, op één locatie draaien met verminderde capaciteit en performance;
- Servers worden dagelijks veiliggesteld door een back-up door middel van snapshots en worden in de Azure cloud opgeslagen. Bij de back-up bestanden worden dagelijks de transactielogs bewaard. Recovery Point Objective¹⁹ = < 2 uur, Recovery Time Objective²⁰ = < 12 uur;

¹⁶ Volgens artikel 22 lid 1 AVG is “een uitsluitend op geautomatiseerde verwerking” verboden.

¹⁷ 240130 Backup en restore document versie 1.3.pdf

¹⁸ Hostingpartij Interconnect zie hoofdstuk 8.4 [Subverwerkers van Xedule](#).

¹⁹ RPO is de tijdsduur die aangeeft hoeveel gegevens er verloren kunnen gaan voordat het herstelproces begint.

²⁰ RTO is de tijdsduur die aangeeft hoe snel een systeem of dienst na een storing weer operationeel moet zijn.

- Databases met klantdata worden dagelijks veiliggesteld. Recovery Point Objective = < 2 uur, Recovery Time Objective = < 12 uur;

7.4 Pseudonimiseren

Xedule pseudonimiseert de verzamelde feedback data (customer satisfaction score) via pNPS (zie 8.3.1 Verbeteren van dienstverlening en applicatie). Deze gegevens worden ontdaan van persoonsgegevens voordat ze in een ‘big data’ oplossing worden verwerkt. Hierdoor kunnen de analisten deze gegevens niet herleiden naar natuurlijke personen. De betrokkene achter de uitvraag is enkel terug te vinden als Xedule de informatie weer combineert. Hiervoor zijn meerdere personen noodzakelijk zijn omdat geen individueel persoon toegang heeft tot zowel de originele data als de gepseudonimiseerde data. De instellingen en de gebruikers kunnen via een opt-out afzien van deze verwerking (meer in hoofdstuk 18.17 Heridentificering gepseudonimiseerde pNPS-gegevens).

7.5 Anonimiseren / pseudonimiseren

De onderwijsinstelling kan, als verwerkingsverantwoordelijke, via het ticketsysteem van Xedule een verzoek tot anonimiseren indienen. Daarna wordt een kopie van de productiedatabase naar een testomgeving overgezet en wordt het anonimiseringscript door een developer van Xedule uitgevoerd. Dit script vervangt namen, e-mailadressen en student- of docentnummers door gefingeerde waarden.

Hoewel deze methode de herkenbaarheid van enkele directe persoonsgegevens kan verminderen, leidt dit niet tot daadwerkelijke anonimisering. De dataset voldoet aan de eisen voor anonimisering zoals bedoeld in de AVG, maar zal eerder als pseudonimisering worden beschouwd (meer in hoofdstuk 18.16 Heridentificering van gepseudonimiseerde gegevens door gebrekkige **anonimiseringsmethode**).

7.6 Encryptie

7.6.1 Encryptie data in transit

Bij het verwerken (persoons)gegevens in transit wordt encryptie ingezet. Dit betekent dat alle communicatie tussen systemen altijd plaatsvindt via een beveiligde verbinding, met HTTPS en het onderliggende TLS-protocol (Transport Layer Security); TLS 1.2. Er is een project gedefinieerd om over te stappen naar TLS 1.3 hier is door Xedule nog geen planning van bekend gemaakt. De beveiliging van deze verbindingen wordt geborgd door technische en organisatorische maatregelen:

- Elk kwartaal wordt gecontroleerd of de SSL Labs-rating minimaal op niveau A staat. Dit houdt in dat de TLS-configuratie voldoet aan actuele best practices, waaronder het gebruik van sterke cipher suites en het correct instellen van HTTP Strict Transport Security (HSTS).

- Periodiek worden de certificaten gecontroleerd op de geldigheid en wordt de volgorde van de geaccepteerde ciphers zo ingesteld dat de sterkste algoritmen als eerste worden aangeboden.
- Beheer van encryptie en certificaten is in beheer bij Xedule.

7.6.2 Encryptie data at rest

7.6.2.1 Database

Op dit moment is de database (DB) nog niet voorzien van encryptie. Om dit te realiseren is binnen Xedule een project opgestart. Voor de implementatie en optimalisatie van encryptie en andere beveiligingsmaatregelen wordt door Xedule een gespecialiseerde database-expert ingeschakeld. Hiervoor heeft Xedule nog geen planning bekend gemaakt.

7.6.2.2 Storage

De database en het volledige platform draaien op een HP Storage-systeem dat is uitgerust met redundante hardware in een dubbel datacenter-opzet. De encryptie van data at rest is op deze storage-systemen hardware matig geregeld volgens de FIPS 140-2-standaard, waarbij gebruik wordt gemaakt van AES-256 encryptie. Hierdoor wordt data die op de schijven is opgeslagen automatisch versleuteld. Mocht een schijf uitgeschakeld, defect of uit de redundantie verwijderd worden, dan wordt deze direct gelocked, zodat de data niet toegankelijk is voor onbevoegden.²¹ Het sleutelbeheer voor deze hardware matige encryptie is ingebouwd in de storage-unit en wordt beheerd door Xedule.

7.6.2.3 Backup

Back-ups van de data worden op meerdere fysieke locaties opgeslagen. Back-ups worden bewaard op de eerdergenoemde storage-units (lokaal), waardoor deze automatisch hardwarematig encrypted zijn. Daarnaast worden back-ups off-site opgeslagen in Microsoft Azure, waar eveneens encryptie wordt toegepast. Dit is aangetoond door de ontwikkelaar tijdens een pilot-audit voor de SURF security baseline. Daarnaast wordt versiebeheer toegepast op de back-ups in Azure, zodat besmetting met bijvoorbeeld ransomware kan worden voorkomen en herstel naar een eerdere, niet-gecompromitteerde versie mogelijk blijft.

7.7 API's

7.7.1 Gestandaardiseerde integratiemogelijkheden

In de onderstaande tabel zijn de integratiemogelijkheden weergegeven. Het doelsysteem is hierbij de aanvrager van deze gegevens via de door het bronsysteem aangeboden API's. Het aanvraagtype staat voor de aanvraag die door het doelsysteem bij het bronsysteem wordt gedaan, waarbij GET staat voor informatie ophalen.

²¹ HPE Storage Security: <https://www.hpe.com/psnow/doc/a00050848enw>.

Bronstelsysteem	Aanvraag	Gegevens	Doelsysteem
AFAS	GET	AFAS-gegevens klant	Xedule
Eduarte	GET	Eduarte-gegevens klant	Xedule
Osiris	GET	Osiris-gegevens klant	Xedule
HR2day	GET	HR2day-gegevens klant	Xedule
Magister	GET	Magister-gegevens klant	Xedule
Somtoday	GET	Somtoday-gegevens klant	Xedule
My Xedule	GET	Beschikbaarheid docenten, inschrijvingen studenten	Xedule

Tabel 7-7-1, Aan Xedule te koppelen standaard integraties

7.7.2 Delen

Om data op te kunnen halen uit Xedule, zijn momenteel de volgende API's beschikbaar:

1. Xedule REST API

Deze API wordt momenteel het meest gebruikt door instellingen en was tot januari 2025 de meest recente API. De gegevensuitwisseling gaat via JSON ten opzichte van XML bij SOAP API.

Alle gegevens die een eindgebruiker met de hoogste rechten in de Graphical User Interface GUI van Xedule kan inzien, zoals een functioneel beheerder, vallen onder de scope van wat er is op te halen met deze API. Andere gegevens kunnen dus niet opgehaald worden door deze API.

De beheerder van de API kan verder alleen instellen of een gebruiker lees- en/of schrijfrechten krijgt op de gegevens die hij benadert met de API. Het is voor de beheerder niet mogelijk om onderscheid te maken tussen de gegevens waar een gebruiker toegang toe krijgt. Met andere woorden, gebruikers van de API hebben toegang tot alle data in Xedule die binnen scope vallen. Authenticatie vindt plaats met een API key. Meer in *hoofdstuk 18.14 Verlies van vertrouwelijkheid door Xedule rest API*.

2. Xedule Management SOAP API

Dit is een verouderde (deprecated) API die nog door enkele instellingen wordt gebruikt. Hieraan worden geen nieuwe functies toegevoegd. Xedule stelt dat de beveiliging hiervan nog wel wordt onderhouden. In principe functioneert deze API hetzelfde als de Xedule REST

API, maar gegevensuitwisseling vindt plaats via XML, in plaats van via JSON met de REST API. Meer in *hoofdstuk 18.15 Verlies van vertrouwelijkheid en controle door ongeautoriseerde toegang door verouderde SOAP API*.

3. Xedule Connect

Connect is een nieuw API-beheersplatform gebouwd op basis van Microsoft Azure API Management en is vanaf januari 2025 in productie gegaan. Zoals de vorige twee API's, dient Connect als een manier om gegevens uit Xedule op te halen. Het grote verschil met de voornoemde API's is dat authenticatie naar de in Connect aangemaakte API's verloopt via OAuth 2.0. De verleende toegang tot data binnen Xedule kan daarnaast ingesteld kan worden met behulp van standaard gedefinieerde rollen. Xedule stelt dat een ander bijkomend voordeel in de toekomst is dat het beheer van API-keys zelf gedaan kan worden, in plaats van handmatige aanvragen via de ontwikkelaars van Xedule. Daarnaast komt op termijn logging beschikbaar op het Connect ontwikkelaarsportaal. Ten tijde van publicatie van deze DPIA zijn er nog geen gebruikers van Connect.

4. Notificaties

Naast API's om data op te kunnen halen, zijn er ook API's beschikbaar waarmee een klant notificaties kan krijgen bij wijzigingen in bepaalde gegevens in Xedule. Bijvoorbeeld als een student zich heeft ingeschreven voor een toets.

In totaal stelt Xedule 4 verschillende API's beschikbaar.

Bronstelsysteem	API	Primair doel	Logging	Authenticatie
Xedule	Xedule REST API	Data ophalen uit Xedule. Zelfde data als beschikbaar via de GUI.	Handmatig verzoek aan Xedule ontwikkelaars	API Key
Xedule	Xedule Management SOAP API (verouderd)	Data ophalen uit Xedule. Zelfde data als beschikbaar via de GUI.	Handmatig verzoek aan Xedule ontwikkelaars	API Key
Xedule	Xedule Connect (in ontwikkeling)	Data ophalen uit Xedule. Zelfde data als beschikbaar via de GUI.	Op termijn zelf in te zien in de ontwikkelaars-portaal	OAuth 2.0

Xedule	Xedule Notification Service	Bij wijzigingen in Xedule geautomatiseerd berichten versturen.	Handmatig verzoek aan Xedule ontwikkelaars	OAuth 2.0
--------	-----------------------------	--	--	-----------

Tabel 7-7-2, Aangeboden standaard API's binnen Xedule

Naast dat er API's beschikbaar zijn waarmee bijvoorbeeld ontwikkelaars van instellingen maatwerk kunnen bouwen, kan Xedule ook terugzenden naar systemen die al gekoppeld zijn om data te ontvangen, zie hoofdstuk 6.1.1 Geautomatiseerde verzameling. Dit verloopt dan via dezelfde endpoints als bij de GET-aanvragen in Tabel 7-7-1, Aan Xedule te koppelen standaard integraties. In de onderstaande tabel staat dit aangegeven. Hierbij staat POST voor informatie toezendend vanuit het bronsysteem naar het doelsysteem.

Bronstelsysteem	Doelsysteem	Aanvraag	Gegevens
Xedule	Eduarte	POST	Subset van groepen inclusief studentrelaties met de groepen
Xedule	Eduarte	POST	Beschikbare roosters in Xedule
Xedule	Osiris	POST	Beschikbare roosters in Xedule
Xedule	Osiris	POST	Subset van groepen inclusief studentrelaties met de groepen
Xedule	Somtoday	POST	Beschikbare roosters in Xedule

Tabel 7-7-3, Aan Xedule te koppelen standaard integraties met doorgiftemogelijkheden

7.7.2.1 |My Xedule| Graph API

Met de Graph API kun je agenda's en gebeurtenissen creëren, lezen, bijwerken en verwijderen binnen Microsoft Outlook (Microsoft Exchange). Dit geldt voor zowel individuele als gedeelde agenda's en ondersteunt ook terugkerende afspraken en tijdzones. Ook is het hiermee mogelijk om automatisch Microsoft Teams meetings te koppelen aan Xedule lessen.

Outlook (Exchange) krijgt dan leesrechten om de afspraken in de (Xedule) feed te zien en te vergelijken met de bestaande afspraken in de third party applicatie zodat er geen dubbele afspraken in komen te staan.

Permission type

Permissions (from least to most privileged)

Application	Calenders.Read
Application	Calenders.ReadWrite
Application	MailboxSettings.Read
Delegated	User.Read
Application	User.Read.All

Tabel 7-7-4

7.8 Cookies

Cookies zijn kleine tekstbestanden die door het bezoek aan een Xedule en/of My Xedule op een apparaat worden geplaatst om (persoons)gegevens op het device van de gebruiker op te slaan.

7.8.1 Xedule

Xedule maakt gebruik van twee functionele cookies. Deze cookies worden lokaal in de browser van de gebruiker opgeslagen. Beide cookies hebben betrekking op het faciliteren van de authenticatie.

Naam cookie: **ASP.NET_SessionId**

Bewaartermijn: sessie

Deze cookie bevat een gepseudonimiseerde identifier die door Xedule gebruikt wordt om de gebruikerssessie te beheren binnen de (ASP.NET) applicatie. De cookie is noodzakelijk voor het bijhouden van de authenticatiestatus. Deze identifier wordt gekoppeld aan server-side opgeslagen sessiegegevens.

Naam Cookie: **Target**

Bewaartermijn: sessie

Dit is een sessie-cookie die door Xedule wordt gebruikt voor het bijhouden van sessie-specifieke doelen of voorkeuren binnen de applicatie.

7.8.2 My Xedule

My Xedule maakt gebruik van vijf functionele cookies. Deze cookies worden lokaal opgeslagen in de browser van de gebruiker. Vier van deze cookies worden gebruikt voor Quality Control via Azure Application Insights, waarmee de technische prestaties en gebruikerservaring van de applicatie worden gemonitord. Zie ook **Fout! Verwijzingsbron niet gevonden.** De vijfde cookie betreft een sessie-identificatie (ASP.NET SessionId) die wordt gebruikt voor het authenticatieproces.

ai_session²²

Bewaartermijn: 30 minuten

Deze cookie wordt gebruikt om een unieke sessie bij te houden binnen Azure Insights. Het helpt bij het groeperen van gerelateerde activiteiten tijdens één bezoek aan de website.

ai_user²³

Bewaartermijn: ~1 jaar (308 dagen)

Deze cookie bevat een gepseudonimiseerde identifier die door Azure Application Insights wordt gebruikt om gebruikersinteracties over langere tijd te kunnen analyseren. Deze identifier wordt gekoppeld aan technische gegevens over het gebruik van de applicatie en moet daarom behandeld worden als persoonsgegevens.

ARRAffinity en ARRAffinitySameSite²⁴

Bewaartermijn: sessie

Deze twee cookies werken samen en zijn specifiek voor Azure's Application Request Routing.

ASP.NET_SessionId

Bewaartermijn: sessie

Deze cookie bevat een gepseudonimiseerde sessie-identifier die gebruikt wordt om de gebruikerssessie te beheren binnen de (ASP.NET) applicatie. De cookie is noodzakelijk voor het bijhouden van de authenticatiestatus. De identifier wordt gekoppeld aan server-side opgeslagen sessiegegevens.

²² Microsoft Cookie Compliance - <https://learn.microsoft.com/en-us/dynamics365/commerce/cookie-compliance>

²³ Microsoft Cookie Compliance - <https://learn.microsoft.com/en-us/dynamics365/commerce/cookie-compliance>

²⁴ Microsoft Azure: ARRAffinity - <https://learn.microsoft.com/en-gb/archive/blogs/devschool/azure-arraffinity-makes-affinity-cookies>

8 Betrokken partijen

Om de rechtmatigheid van de gegevensverwerkingen te kunnen beoordelen, moet inzichtelijk zijn welke partijen betrokken zijn bij welke gegevensverwerking en in welke hoedanigheid: verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker, sub-verwerker, verstrekker of ontvanger.²⁵

Voor het kwalificeren van de AVG-rol van een partij zijn de juridische verhoudingen niet doorslaggevend, maar moet de feitelijke situatie beoordeeld worden. De juridische rolverdeling, onder andere vastgelegd in de verwerkersovereenkomst kan wel meegenomen worden in de afweging. Partijen kunnen meerdere AVG-rollen tegelijk hebben, bijvoorbeeld wanneer de onderwijsinstelling als verwerkingsverantwoordelijke ook een verstrekker is. Het is niet mogelijk om zowel verwerker en verwerkingsverantwoordelijke tegelijkertijd te zijn voor *dezelfde gegevensverwerking*. Elke verwerking van persoonsgegevens heeft minimaal een verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan, die het doel van en de middelen voor de gegevensverwerkingen vaststelt.²⁶ De verwerker is de partij die persoonsgegevens alleen ten behoeve van de verwerkingsverantwoordelijke verwerkt.²⁷ Hieronder worden diverse rollen nader toegelicht.

8.1 Onderwijsinstelling: Verwerkingsverantwoordelijke

Instellingen zijn de verwerkingsverantwoordelijken voor de gegevensverwerkingen ten behoeve van de onderwijsplanning en roostering binnen Xedule en My Xedule. Ook zijn instellingen verantwoordelijk voor de verwerkingen die noodzakelijk zijn om onderwijsplanning en roostering in de applicaties mogelijk te maken. Dit zijn identificatie- en authenticatieverwerkingen, het maken van back-ups, het personaliseren van de applicaties en de applicatielogging die gebruikt wordt om de applicatie te onderhouden en beveiligen (zie hoofdstuk 6 Gegevensverwerkingen). Hoewel een verwerker in de praktijk zelf de niet-essentiële middelen kiest waarmee de verwerkingen worden uitgevoerd, en Xedule als SaaS-dienstverlener werkt met haar eigen ontwikkelde softwaredienst, is het uiteindelijk de onderwijsinstelling die als verwerkingsverantwoordelijke besluit om Xedule en My Xedule in te zetten voor het onderwijslogistieke proces. Zij bepalen waarvoor de persoonsgegevens van studenten en medewerkers verwerkt worden, in welke mate en op welke manier. Dit maakt hen verantwoordelijk.

²⁵ De Autoriteit Persoonsgegevens heeft een tabel gepubliceerd met voorbeelden van situaties en uitleg welke organisatie in die situaties welke rol uitoefenen. (<https://www.autoriteitpersoonsgegevens.nl/documenten/voorbeeldlijst-wie-is-hier-de-verwerker-en-wie-de-verantwoordelijke>) ⁶⁷ Artikel 4, zevende onderdeel, AVG en artikel 3, onderdeel 8, Richtlijn.

²⁶ Artikel 4 sub 7 van de AVG.

²⁷ Artikel 4 sub 8 van de AVG.

8.2 Xedule: Verwerker

Xedule, als eigenaar en aanbieder van Xedule en My Xedule, is de verwerker voor alle verwerkingen die onder 8.1 genoemd zijn. Xedule is namelijk de rechtspersoon die persoonsgegevens verwerkt in opdracht van de onderwijsinstelling(en) en conform diens instructies.

De afspraken hieromtrent zijn vastgelegd in de verwerkersovereenkomst die Xedule standaard aanbiedt, gebaseerd op model Verwerkersovereenkomst versie 3.0, SURF Juridisch Normenkader (Cloud)services. In de bijlage zijn de verwerkingsactiviteiten die bij Xedule worden belegd beschreven op een algemene manier. Dezelfde groep van vijftien verwerkingsactiviteiten wordt per product beschreven en er is geen koppeling tussen de doeleinden, de verwerkingen die Xedule in opdracht van de instellingen uitvoert en de persoonsgegevens die hiervoor verwerkt worden. De verwerkersovereenkomst biedt dan ook beperkte houvast voor de kwalificatie van Xedule als verwerker voor specifieke verwerkingen, waardoor er vooral naar de feitelijke situatie is gekeken.

8.3 Xedule: Verwerkingsverantwoordelijke

Xedule voert volgens haar privacy statement verwerkingen als verwerkingsverantwoordelijke uit met persoonsgegevens van gebruikers van Xedule en My Xedule voor het verbeteren van de dienstverlening of de applicatie en voor marketing en communicatie. Daarnaast voert Xedule volgens het loggingbeleid systeemlogging uit “om te voldoen aan verzoeken van betrokkenen, analyses rondom informatiebeveiliging/datalekken en foutanalyses.”

8.3.1 Verbeteren van dienstverlening en applicatie

De methode die Xedule gebruikt voor het verbeteren van de dienstverlening is onder andere het uitvoeren van klanttevredenheidsonderzoeken door middel van een Product Net Promoter System (pNPS). Xedule vraagt hiervoor gebruikers' meningen in de applicaties aan de hand van klanttevredenheidsvragen en slaat deze informatie volgens het privacy statement anoniem op. Gebruikers kunnen aangeven dat ze niet mee willen doen, waarna ze een jaar niet opnieuw benaderd worden. Ook worden de klanttevredenheidsonderzoeken niet uitgevoerd als een instelling aangeeft geen deel te willen nemen aan de onderzoeken. Het privacy statement beschrijft niet:

- Welke andere methodes Xedule gebruikt om gegevens te verzamelen ten behoeve van de verbetering van de dienstverlening.
- Welke grondslag Xedule hanteert voor pNPS.
- Welke persoonsgegevens Xedule verzamelt.
- Hoe Xedule de anonimisering van de persoonsgegevens garandeert. In het privacy statement wordt aangegeven dat gebruikers op een later tijdstip kunnen aangeven

dat ze niet meer mee willen doen. Als hun persoonsgegevens geanonimiseerd zouden zijn, zou het echter niet mogelijk zijn om hun deelname in te trekken.

- Welke bewaartermijnen Xedule hanteert.
- Welke partijen de gegevens ontvangen. Wel is er op de website van Xedule te vinden dat de aangeraden pNPS tool InMoment is.²⁸ Het is niet duidelijk of InMoment een verwerker of een verwerkingsverantwoordelijke is.
- Of er doorgifte van de gegevens plaatsvindt. Wel is bekend dat InMoment gevestigd is in de Verenigde Staten.²⁹

Uit het loggingbeleid blijkt ook dat er systeemlogging plaatsvindt van “Geaggregeerde informatie ten behoeve van monitoring op hard- en software prestaties” ten behoeve van het verbeteren van het platform. Deze verwerkingen vinden plaats in Azure Insights en Xedule heeft aangegeven dat de namen van gebruikers gekoppeld worden aan deze informatie. Xedule verstrekt verder geen informatie over deze verwerkingen, niet in de documentatie en niet in de inzageverzoeken.

De instellingen hebben zelf niet het doel en de middelen van deze verwerkingen bepaald en de verwerkingen die plaatsvinden ten behoeve van deze doeleinden zijn niet in hun belang. Hoewel het verbeteren van de applicatie wel in de verwerkersovereenkomst als doel genoemd wordt, is niet beschreven dat en hoe systeemlogging plaatsvindt ten behoeve van dit doel. Instellingen hebben niet voldoende inzicht in de verwerkingen om hiermee als verwerkingsverantwoordelijke mee in te kunnen stemmen. Daarom moet Xedule als verwerkingsverantwoordelijke voor bovenstaande verwerkingen gekwalificeerd worden.

8.3.2 Systeemlogging voor betrokkeneverzoeken, foutanalyses en analyses rondom informatiebeveiliging en datalekken

Uit het loggingbeleid blijkt dat Xedule systeemlogging uitvoert voor een aantal doeleinden, die (naast verbetering van de dienstverlening, zie 8.3.1) aan de hand van de verstrekte informatie kunnen worden samengevat als fraudepreventie en beveiliging. Waar instellingen zeggenschap hebben over de applicatielogging, omdat deze inzichtelijk is voor beheerders in de applicatie zelf, geldt dit niet voor de systeemlogging. Instellingen hebben geen manier om inzage te krijgen in de systeemlogging naast het loggingbeleid. Het loggingbeleid is echter incompleet, omdat alleen de belangrijkste loggingitems beschreven worden. Verder wordt er enkel op hoofdlijnen beschreven welke soorten logging plaatsvinden en wat het algemene doel van elk type logging is. De feitelijk gelogde gegevens zijn op hoog niveau gecategoriseerd en het is niet duidelijk of er pseudonimisering plaatsvindt in het loggingproces. Daarnaast is de toegang tot de logs summier beschreven, zonder duidelijke vermelding van autorisatieprocedures of toegangsbeperkingen. In de basis bewaard Xedule deze logs 6 maanden vanaf verzamelen voor productie omgevingen.

²⁸ <https://ux.Xedule.com/ux-in-Xedule/methods/product-nps-pnps>, geraadpleegd op 30 april 2025.

²⁹ <https://inmoment.com/privacy-policy/>, geraadpleegd op 30 april 2025.

Hoewel de instellingen wel een belang hebben bij een goede beveiliging van de applicaties, is het dus feitelijk niet mogelijk voor deze om het doel en de middelen van de systeemlogging te bepalen. Het is namelijk niet inzichtelijk is wat voor logging er plaatsvindt, hoe de logging is ingericht en welke afwegingen er zijn gemaakt. Deze verwerkingen worden ook niet beschreven in de verwerkersovereenkomst. Daarom moet Xedule voor deze verwerkingen als verwerkingsverantwoordelijke worden gekwalificeerd.

8.3.3 Marketing en communicatie

Xedule geeft in het privacy statement aan: “Door gebruik te maken van de applicatie van Xedule kan en mag Xedule de verzameling van persoonsgegevens gebruiken voor relevante marketing en communicatie.” Welke persoonsgegevens dit zijn, wie er worden benaderd, hoe mensen worden benaderd en hoe de afweging voor het gerechtvaardigd belang van Xedule eruit ziet wordt niet beschreven. Marketing en communicatie zijn ook doelen die Xedule zelf heeft bepaald, niet in de verwerkersovereenkomst worden genoemd en niet in het belang van de instellingen zijn. Xedule is dus verwerkingsverantwoordelijke voor verwerkingen van de persoonsgegevens van Xedule en My Xedule gebruikers voor deze doelen.

8.4 Subverwerkers van Xedule

De subverwerker is de natuurlijke persoon, rechtspersoon of overheidsorgaan die ten behoeve van de verwerker specifieke taken uitvoert in het kader van de samenwerking tussen de verwerker en de verwerkingsverantwoordelijke.³⁰ Een subverwerker is dus de verwerker van de verwerker.³¹

Xedule maakt - ten behoeve van de gegevensverwerking van de instellingen - gebruik van de diensten van subverwerkers. De subverwerkers vallen onder de verantwoordelijkheid van Xedule en deze dienen daarbij dezelfde verplichtingen te worden opgelegd als Xedule opgelegd heeft gekregen van de verwerkingsverantwoordelijke (de onderwijsinstelling) in de verwerkersovereenkomst.

Toestemming subverwerkers in verwerkersovereenkomst

Xedule dient als verwerker schriftelijke toestemming te vragen aan de onderwijsinstelling om gebruik te mogen maken van een subverwerker. Deze verplichting is vastgelegd in de verwerkersovereenkomst. In overeenstemming met artikel 28 lid 2 en 4 van de AVG is in deze verwerkersovereenkomst expliciet vastgelegd dat de inzet van subverwerkers uitsluitend plaatsvindt na voorafgaande specifieke toestemming van de onderwijsinstelling.

³⁰ Artikel 28, lid 2 van de AVG.

³¹ Verwerkingsverantwoordelijke of gegevensverwerker | European Data Protection Board

Overzicht subverwerkers

In de Verwerkersovereenkomst is een overzicht opgenomen met subverwerkers waarvan Xedule gebruik maakt. Gebleken is dat deze lijst met subverwerkers niet volledig en niet meer actueel is waardoor er geen correcte weergave van de huidige situatie wordt geschetst. Uit de gesprekken die hierop volgden heeft Xedule een geactualiseerd overzicht aangeleverd, dat in tabel 8-1 beschikbaar wordt gesteld. Het geactualiseerde overzicht is nog niet in de overeenkomst verwerkt.

Hieronder volgt een specificatie van de subverwerkers die door Xedule zijn ingeschakeld, en die mogelijk toegang kunnen krijgen tot de persoonsgegevens (studenten en medewerkers) van de onderwijsinstelling.

Subverwerker + locatie	Opslag - locatie	Xedule of My Xedule	Uitgevoerde diensten	Contractuele waarborgen gegevensbescherming aanwezig?	
				Organisatorisch en juridisch	Technisch en fysiek
Atlan (NL)	EER/NL	Xedule	Cloudbeheer en bewaking van de opslag van cloud-infrastructuur	Inbegrepen in algemene voorwaarden Atlan	Nee
Escrow4All (NL)	EER/NL	Xedule en My Xedule	Beheer SaaS-omgeving en opslag t.b.v. continuïteit	Verwerker-subverwerker overeenkomst	Nee
Synaxion (NL)	EER/NL	Xedule	Dashboarding	Nee	Nee
Microsoft Azure (VS)	EER	My Xedule	Cloudopslag	Standaard DPA Microsoft	Ja
InMoment	Niet bekend	Niet bekend	Niet bekend	Niet bekend	Niet bekend

Tabel 8-1

Contractuele waarborgen subverwerkers

Xedule heeft de hoofdovereenkomsten waar de gegevensbeschermingsafspraken bij horen niet geleverd. Het is dus niet duidelijk welke verwerkingen bij de subverwerkers belegd zijn en wat de kenmerken hiervan zijn. Daarom gaat deze DPIA ervan uit dat de subverwerkers alle persoonsgegevens kunnen verwerken die Xedule verwerkt.

Ook bevatten de afspraken met Xedule's subverwerkers geen eigen lijst met subverwerkers en bevat een deel geen (appendix met) technische maatregelen die worden toegepast ter bescherming van de persoonsgegevens.

Verder verschillen een aantal bepalingen in de contracten met de subverwerkers van de bepalingen in de SURF Modelverwerkersovereenkomst, waaronder de verplichting om alleen met toestemming van verwerkingsverantwoordelijke nieuwe subverwerkers in te schakelen.

Ontbrekende documentatie

Van InMoment is er geen documentatie beschikbaar. Tussen Xedule en Synaxion is er wel een overeenkomst, maar hierin is Synaxion verwerker en Xedule subverwerker.

8.5 Betrokkenen

Xedule en My Xedule onderscheiden drie categorieën betrokkenen bij de gegevensverwerkingen. De eerste twee categorieën zijn de eindgebruikers van My Xedule en de laatste categorie zijn de medewerkers die de roosters opstellen, wijzigen, goedkeuren enzovoorts.

- 1) Studenten onderwijsinstelling (aankomende studenten, studenten, oud student)
- 2) Docenten (docent, instructeur, onderwijsassistent, examinatoren)
- 3) Medewerkers onderwijsinstelling (roosteraar, leidinggevende, team coördinator, staf, systeembeheerder)

8.6 Ontvangers

De ontvangers van persoonsgegevens zijn medewerkers die toegang hebben tot het roosteringsysteem en de studenten die hun eigen rooster kunnen inzien. Daarnaast behoren de eerdergenoemde subverwerkers tot de ontvangers, alsmede als onderstaande derden.

8.7 Verstrekkers

Zowel de onderwijsinstelling als Xedule zijn verstrekkers van persoonsgegevens; de onderwijsinstelling verstrekt persoonsgegevens aan Xedule en Xedule verstrekt gegevens aan haar subverwerkers en derden.

8.8 Derden

Externe partijen die mogelijk toegang krijgen tot (geanonimiseerde / geaggregeerde) roosteringsgegevens. Denk aan (beheerders) van cloudhostingpartijen, zoals Interconnect, maar ook overheidsinstanties zoals onderwijsinspectie en/of de arbeidsinspectie.

Interconnect

Xedule gebruikt Interconnect als colocatiedienst en is eigenaar van de servers die bij Interconnect staan. Deze servers bevatten de gegevens van Xedule en My Xedule. Xedule stelt Interconnect geen opdracht te hebben gegeven om enige verwerking uit te voeren met betrekking tot de persoonsgegevens die op de servers staan, waaronder het maken van back-ups. De diensten van Interconnect bestaan er slechts uit zorg te dragen voor de fysieke omstandigheden die voorwaardelijk zijn voor het functioneren van de servers. Xedule heeft de hoofdovereenkomst tussen Xedule en Interconnect niet geleverd, dus deze stellingen zijn niet gecontroleerd.

De servers staan in een afgesloten ruimte, waar Interconnect wel toegang toe heeft als zij een inspectie uitvoeren of als onvoorziene omstandigheden Interconnect dwingen om apparatuur te verplaatsen, uit te schakelen of verwijderen.

9 Belangen bij de gegevensverwerkingen

9.1 Onderwijsinstelling

Als onderwijsinstelling, en daarmee verwerkingsverantwoordelijke, heeft zij diverse belangen bij een zorgvuldige organisatie van het onderwijslogistieke proces. Deze belangen, zoals een efficiënte planning/rooster en waarborgen van persoonsgegevens, sluiten aan bij de wettelijke en publieke taken zoals vastgelegd in de Wet educatie en beroepsonderwijs (WEB) en de Wet op het Hoger Onderwijs en Wetenschappelijk onderzoek (WHW). :

- **Zorgvuldige omgang van persoonsgegevens:** De onderwijssector kent omstandigheden en uitdagingen die de gevoeligheid van de verwerking van persoonsgegevens in een roosterapplicatie kunnen vergroten. Instellingen hebben daarom een groot belang bij een goed verloop van dit onderwijslogistiekproces, waarbij de focus ligt op het bieden en onderhouden van een veilige leer- en werkomgeving waarin de zorgvuldige omgang van student- en medewerkersgegevens geborgd blijft.
- **Efficiënte planning en roosters:** De inzet van Xedule helpt instellingen om het onderwijslogistieke proces efficiënter te beheren en optimaliseren.
- **Kwaliteit van het onderwijs en de organisatie:** Het gebruik van Xedule kan bijdragen aan een efficiëntere coördinatie van lessen en werklasten. Daarnaast wordt de wendbaarheid vergroot doordat instellingen sneller kunnen anticiperen op onvoorziene omstandigheden. Dit bevordert de kwaliteit van het onderwijsaanbod, evenals een efficiënte inzet van middelen zoals docenten en locaties.
- **Sturingsinformatie:** Xedule beschikt over rapportage-modules die kunnen bijdragen aan strategische besluiten, zoals optimalisatie van werkprocessen en inzet van personeel en locaties.

9.2 Studenten

- **Efficiënte planning en roosters** bieden studenten de mogelijkheid optimaal gebruik te maken van de mogelijkheden van een Gepersonaliseerde leeromgeving waardoor zij in staat zijn om hun studie beter te plannen en af te stemmen op hun eigen behoeften.
- **Zorgvuldige omgang van persoonsgegevens:** Als gebruikers van Xedule en/of My Xedule hebben de studenten er belang bij dat hun persoonsgegevens enkel worden verwerkt voor legitieme doelen en dat deze beschermd zijn tegen ongeoorloofde toegang. Dit belang wordt vergroot nu zij geen inspraak hebben om wel of geen gebruik te maken van de applicaties. Het gebruik ervan is namelijk de keuze van de onderwijsinstelling.

9.3 Medewerkers (Docenten)

- Efficiënte planning en roosters zorgen voor evenwichtige spreidingen van lessen, vergadermomenten en nakijkmomenten, waardoor onnodige piekbelasting kan worden voorkomen. Hierdoor kunnen docenten efficiënt worden ingepland.
- Zorgvuldige omgang van persoonsgegevens: Evenals de studenten, zijn medewerkers (i.c. docenten) gebaat bij de verwerking van hun persoonsgegevens enkel voor legitieme doelen en bescherming tegen ongeoorloofde toegang.

9.4 Xedule

- Leveren van betrouwbare, kwalitatieve en compliant software om de marktpositie te behouden, dan wel verbeteren.
- Xedule heeft een commercieel belang bij het behouden en verbeteren van haar marktpositie in de Nederlandse onderwijs- en onderzoekssector.

10 Verwerkingslocaties

Xedule en My Xedule zijn een SaaS-oplossing van Xedule, wat betekent dat de persoonsgegevens die via deze applicaties worden verwerkt, terechtkomen in de cloudomgeving van Xedule.

Xedule maakt gebruik van de datacenters van Interconnect welke zijn gevestigd in de EER. Xedule en My Xedule worden geleverd vanuit de Nederlandse datacentra in Eindhoven en Den Bosch. Het beheer en inrichting van deze datacenters is belegd bij Atlan, eveneens gevestigd in Nederland.

Xedule maakt gebruik van Microsoft Azure Monitor Application Insights om gebruik en prestaties van My Xedule te loggen en monitoren. Hierbij worden gegevens verwerkt, zoals welke applicaties gebruikers gebruiken, wat hun webbrowser is, responstijden en op welke tijdstippen ze applicaties gebruiken. Deze gegevens worden gekoppeld aan hun username, waardoor het persoonsgegevens zijn. Het is niet bekend of Xedule voor opslag en verwerking binnen de EU Data Boundary heeft gekozen, of de contractspartij van Xedule binnen of buiten de EER gevestigd is en of de gegevens worden gepseudonimiseerd of geanonimiseerd tijdens de processen.

Ook slaat Xedule een versleutelde back-up op bij Microsoft Azure. Xedule stelt de sleutels hiervoor zelf te beheren.

11 Juridisch en beleidsmatig kader

Hieronder is beschreven welke wet- en regelgeving, naast de AVG, nog meer van toepassing zijn op de gegevensverwerking.

11.1 Juridische en beleidsmatige kaders

Juridisch kader	Artikel	Gegevensverwerkingen
Wet op educatie beroepsonderwijs (WEB)	Diverse artikelen	Registratie van inschrijvingen, studievoortgang en diploma-uitgiften.
Wet op het Hoger onderwijs en Wetenschappelijk onderzoek (WHW)	Diverse artikelen	Registratie van inschrijvingen, studievoortgang en diploma-uitgiften.
Burgerlijk Wetboek (BW)	Artikel 7:611 – Goed werkgeverschap	Correcte administratie rondom inzet- en planning van medewerkers.
Wet op de loonbelasting	Diverse artikelen	Administratie rondom salaris op basis van inzet- en middelenplanning.
Arbeidstijdenwet	Diverse artikelen	Registratie en monitoring van met name verlof en overuren.
Wet op de Ondernemingsraden (WOR)	Art. 27 lid 1 sub K	Implementeren of wijzigen van planning- en roosteringsapplicatie rondom de verwerking van medewerkersgegevens in het kader van werktijden, beschikbaarheid, verzuim en verlof.
Besluit basisregistratie personen (BRP)	Diverse artikelen	Opvragen en verificatie adres- en identiteitsgegevens van studenten en medewerkers.
Telecommunicatiewet	Art. 11.7a	Verzamelen van persoonsgegevens via cookies op de website
Privacybeleid onderwijsinstelling	n.v.t.	Richtlijnen over opslag en gebruik van persoonsgegevens van medewerkers en studenten.

Informatiebeveiligingsbeleid	n.v.t.	Richtlijnen over beheer en (deels) verwerking van informatie (waaronder persoonsgegevens).
------------------------------	--------	--

11.2 Corporate Xedule beleid

Xedule maakt deel uit van Visma Group, een internationaal concern met een overkoepelend strategisch beleid en centrale richtlijnen op het gebied van privacy. Hoewel dochterondernemingen operationele autonomie genieten, is deze vrijheid op het gebied van privacy beperkt. De Visma Group hanteert een uitgebreid Data Protection Programma, waarin beleid, richtlijnen, risicomanagement en verplichte privacytrainingen voor alle medewerkers zijn opgenomen. Dit betekent dat Xedule zich bij de ontwikkeling van Xedule en My Xedule niet alleen conformeert aan externe wet- en regelgeving, zoals de AVG en UAVG, maar tevens aan het corporate beleid en de centrale kaders die door Visma Group zijn vastgesteld.

12 Bewaartermijnen

12.1 Bewaartermijnen als verwerker

Xedule

Xedule heeft in haar verwerkersovereenkomst³² en privacy statement³³ opgenomen dat de onderwijsinstelling als verwerkingsverantwoordelijke de bewaartermijnen vastlegt en haar persoonsgegevens op eigen initiatief dient te verwijderen uit de applicaties. Xedule zal als verwerker onder geen enkel beding op eigen initiatief persoonsgegevens verwijderen, noch automatisch, noch handmatig.

Enkel met een schriftelijke opdracht of vanuit een melding in het supportsysteem kan verwijdering van persoonsgegevens door Xedule voor de beëindiging van de overeenkomst aangevraagd worden. Wanneer de overeenkomst met de onderwijsinstelling ten einde is gekomen, worden alle persoonsgegevens waarvoor geen wettelijke bewaarplicht voor Xedule bestaat, door Xedule binnen zes maanden verwijderd.

Onderwijsinstelling

Instellingen hebben als verwerkingsverantwoordelijke de wettelijke verplichting om persoonsgegevens niet langer te bewaren dan noodzakelijk om de verwerkingsdoeleinden te verwezenlijken. Dat betekent dat instellingen verantwoordelijk zijn voor het beschrijven van de (wettelijke) bewaartermijn en het hebben van een proces omtrent vernietiging/verwijdering.

Het beschrijven en hebben van een proces ligt in het verantwoordelijkheidsgebied van de onderwijsinstelling en valt daarmee buiten de scope van deze DPIA. Wel is gekeken naar de mogelijkheid die Xedule en My Xedule bieden om aan deze wettelijke verplichting te kunnen voldoen.

In Xedule en My Xedule is het niet mogelijk om bewaartermijnen in te stellen voor een regel, item, vrije invulvelden of andere veld waarin persoonsgegevens zijn opgenomen. Het is daardoor niet mogelijk om zelf te bepalen vanaf welk moment een bewaartermijn begint te lopen. Dat betekent dat instellingen handmatig moeten toezien op het tijdig verwijderen van persoonsgegevens conform de interne en externe normen.

Daarnaast bieden Xedule en My Xedule geen geautomatiseerde functionaliteit om persoonsgegevens na het verstrijken van de bewaartermijn te verwijderen. Het ontbreken van een geautomatiseerd verwijderingsmechanisme in Xedule en My Xedule wordt erkend als risico en verder uitgewerkt in onderdeel C (**Fout! Verwijzingsbron niet gevonden.**).

³² SURF Model Verwerkersovereenkomst 3.0.

³³ [241031 Privacy statement Xedule](#)

12.2 Bewaartermijnen als verwerkingsverantwoordelijke

Xedule hanteert eventuele wettelijke bewaartermijnen en heeft een intern beleid voor bewaartermijnen en verwijdering van persoonsgegevens waarvoor zij verwerkingsverantwoordelijke is. Echter, er is geen verdere inzage of toelichting geboden in dit beleid of onderliggende processen, los van de bewaartermijnen in het loggingbeleid, noch is hierop uitsluitel geboden middels de uitgevoerde inzageverzoeken. Hoewel de verantwoordelijkheid voor het uitvoeren van de inzageverzoeken bij de onderwijsinstelling ligt als verwerkingsverantwoordelijke, worden binnen Xedule en My Xedule ook persoonsgegevens van instellingen verwerkt. De verwerker is wel verplicht om de verwerkersverantwoordelijke in staat te stellen verzoeken van betrokkenen af te kunnen handelen. Om die reden is het relevant om dit aspect mee te nemen in de DPIA. Dit wordt erkend als risico en verder uitgewerkt in onderdeel C.

B. Beoordeling rechtmatigheid gegevensverwerkingen

13 Rechtsgrond

Een verwerkingsverantwoordelijke moet een grondslag hebben om persoonsgegevens rechtmatig te kunnen verwerken.³⁴ Dit hoofdstuk behandelt de mogelijke rechtsgrondslagen die gebruikt kunnen worden voor de verwerkingen die in deze DPIA beschreven worden. Er kunnen verschillende grondslagen gelden wanneer een instelling verantwoordelijk is en wanneer Xedule of een andere partij verantwoordelijk is.

13.1 Grondslagen instellingen

Zoals besproken in paragraaf 8.1 zijn de instellingen verantwoordelijk voor de verwerkingen die vallen onder de onderwijsplanning, roostering en ondersteunende verwerkingsactiviteiten die noodzakelijk zijn om deze doelen mogelijk te maken.

Artikel 6, lid 1 onder e van de AVG (Taak van algemeen belang).

Instellingen hebben de wettelijke verplichting om een publieke taak uit te voeren, te weten het organiseren van het onderwijs.³⁵ Om deze taak uit te kunnen voeren moeten instellingen plannings opstellingen en roosters maken en het verwerken van persoonsgegevens is noodzakelijk om dit te kunnen doen. Om een beroep te doen op deze grondslag moeten instellingen een noodzakelijkheidstoets doen om aan te tonen dat de verwerkingen noodzakelijk zijn om hun publieke taak goed te vervullen. Voor het verwerken van gegevens die niet noodzakelijk zijn voor hun publieke taak, kunnen instellingen mogelijk een van onderstaande grondslagen toepassen.

Artikel 6, lid 1 onder a van de AVG (Toestemming)

Voor het verwerken van de locatiegegevens van gebruikers ten behoeve van het reserveren van een lokaal vraagt de instelling toestemming aan de gebruiker via de applicatie. Deze toestemming moet onder andere vrij zijn om geldig te zijn als grondslag onder de AVG. Dit betekent dat de gebruiker geen nadelige gevolgen mag ondervinden van het weigeren van de toestemming, zoals geen ruimtes kunnen reserveren. Instellingen moeten dus gebruikers die hun locatie niet willen delen dus een alternatieve mogelijkheid bieden om ruimtes te reserveren als ze deze grondslag willen gebruiken.

Artikel 6, lid 1 onder b van de AVG (Uitvoeren overeenkomst)

Verwerkingen die niet noodzakelijk zijn voor het uitvoeren van een publieke taak, zijn mogelijk noodzakelijk om een overeenkomst met studenten (bijvoorbeeld een onderwijsovereenkomst) en/of medewerkers (bijvoorbeeld een arbeidsovereenkomst) uit te

³⁴ Art. 6 AVG.

³⁵ Zie art. 23 Grondwet, art. 1.3 WHW en art. 1.3 WEB.

voeren. Ook hier moeten instellingen een noodzakelijkheidstoets uitvoeren om aan te tonen dat het doel van de overeenkomst niet bereikt kan worden zonder de betreffende verwerkingen van persoonsgegevens.³⁶

Artikel 6 lid 1 onder f van de AVG (Gerechtvaardigd belang)

Verwerkingen die niet noodzakelijk zijn voor het uitvoeren van een publieke taak, zijn mogelijk noodzakelijk voor het behartigen van een gerechtvaardigd belang van de instelling. Om deze grondslag te kunnen gebruiken, moet er getoetst worden of instellingen (1) een gerechtvaardigd belang hebben, (2) de verwerking noodzakelijk is om dit belang te behartigen en (3) of de belangen van de instelling zwaarder wegen dan die van de betrokkenen.³⁷

13.2 Grondslagen Xedule

Xedule voert verwerkingen uit met persoonsgegevens van de gebruikers van Xedule en My Xedule die feitelijk en juridisch niet onder verantwoordelijkheid van de instellingen kunnen vallen. Het bedrijf is verwerkingsverantwoordelijke voor deze verwerkingen, zoals beschreven in paragraaf 8.3. Xedule gebruikt de gegevens die ze hebben verkregen doordat de instellingen hun producten afnemen voor verwerkingen die niet onder de instructie van de instellingen vallen. Deze verdere verwerkingen van Xedule zijn alleen rechtmatig als ze volgens de toets van artikel 6 lid 4 AVG verenigbaar zijn met de originele doelen van de instellingen. Deze toets is voor onderstaande verwerkingen uitgevoerd, aan de hand van de volgende factoren:

- a. Ieder verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld, en de doeleinden van de voorgenomen verdere verwerking;
- b. Het kader waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkenen en de verwerkingsverantwoordelijke betreft;
- c. De aard van de persoonsgegevens, met name of bijzondere categorieën van persoonsgegevens worden verwerkt;
- d. De mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkenen;
- e. Het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering.

³⁶ Richtsnoeren 2/2019 betreffende de verwerking van persoonsgegevens op grond van artikel 6, lid 1, onder b), van de AVG in het kader van de verlening van onlinediensten aan betrokkenen, EDPB

³⁷ <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/grondslagen-avg-uitgelegd#grondslag-gerechtvaardigd-belang>, geraadpleegd op 2 mei 2025.

13.2.1 Verbeteren van dienstverlening en applicatie

Xedule verwerkt zowel systeemlogging als pNPS-gegevens voor het verbeteren van de dienstverlening en de applicatie. Deze doeleinden zijn niet vastgelegd in de verwerkersovereenkomst en ook uit de feitelijke situatie blijkt niet dat de instellingen hier instructies voor geven.

Systeemlogging

Zoals beschreven in **Fout! Verwijzingsbron niet gevonden.** en 8.3.1 is weinig bekend over de systeemlogging en de verwerkingen die Xedule doet met de systeemlogginggegevens. Hoewel het verbeteren van de dienstverlening en de applicatie verband zouden kunnen houden met de doeleinden van de instellingen, voor zover de verwerkingen die voor deze doeleinden plaatsvinden in het belang zijn van de instellingen, kan er slecht getoetst worden of er aan de andere voorwaarden wordt voldaan. Er is weinig inzicht in de aard van de verzamelde persoonsgegevens, de waarborgen die zijn getroffen om nadelige gevolgen te voorkomen en wat deze gevolgen zouden kunnen zijn. Aangezien er niet kan worden aangetoond dat deze verwerkingen voldoen aan de toets verenigbare verwerkingen, moet er geconcludeerd worden dat de verwerkingen niet verenigbaar zijn en dat Xedule dus geen grondslag heeft om deze uit te voeren.

pNPS

Xedule verwerkt persoonsgegevens van betrokkenen in de applicaties om ze te kunnen benaderen met klanttevredenheidsvragen en verwerkt vervolgens hun reacties op deze vragen. Ook hier geldt dat verbetering van de dienstverlening en applicatie in principe een doel zou kunnen zijn dat verenigbaar is met de originele doelen van de instellingen. Er bestaan echter onduidelijkheden over de persoonsgegevens die verwerkt worden, waaronder eventuele diagnostische gegevens, over de wijze waarop pseudonimisering wordt ingezet om de privacy van de betrokkenen te waarborgen, over de bewaartermijnen en over eventuele gevolgen en risico's voor betrokkenen. Daarom kan niet geconcludeerd worden dat deze verwerkingen verenigbaar zijn met de doelen van de instellingen.

13.2.2 Fraudepreventie en beveiliging

Ook fraudepreventie en beveiliging kunnen legitieme doelen zijn, waarvan het in de lijn van verwachting van instellingen en betrokkenen kan liggen dat er verdere verwerkingen voor plaatsvinden wanneer ze de applicaties beschikbaar stellen en gebruiken. Met betrekking tot de systeemlogging die Xedule voor deze doeleinden verwerkt geldt echter, zoals beschreven in 13.2.1, dat er slecht getoetst kan worden of er aan de voorwaarden voor een verenigbare verwerking wordt voldaan. Er is weinig inzicht in de aard van de verzamelde persoonsgegevens, de waarborgen die zijn getroffen om nadelige gevolgen te voorkomen en wat deze gevolgen zouden kunnen zijn. Daarom kunnen ook deze verwerkingen niet gekwalificeerd worden als verenigbaar.

13.2.3 Marketing en communicatie

Marketing en communicatie van Xedule als bedrijf zijn geen doelen die verband houden met de doelen waarvoor de instellingen Xedule's applicaties inzet. Daarnaast is er niets bekend over de verwerkingen die Xedule uitvoert met de persoonsgegevens die het bedrijf verzamelt via de applicaties, behalve er nieuwsbrieven en marketinguitingen verstuurd worden, en berichten vanuit de applicatie. Verder heeft Xedule geen directe contractuele relatie met gebruikers van de applicaties en leidt het versturen van marketing tot een verlies van tijd en concentratie voor de ontvanger. Daarom zijn de marketing- en communicatieverwerkingen van Xedule niet verenigbaar met de originele doelen van de instellingen en heeft Xedule geen grondslag.

14 Bijzondere persoonsgegevens

De persoonsgegevens die doorgaans in Xedule en My Xedule worden verwerkt zijn niet aan te merken als bijzondere persoonsgegevens. Toch bestaat er in bepaalde gevallen de mogelijkheid dat er wel persoonsgegevens worden verwerkt in Xedule of My Xedule die specifiek zien op de gezondheid van medewerkers en/of studenten.

Het is volgens artikel 9 AVG verboden om bijzondere persoonsgegevens te verwerken. Dit verbod kan enkel doorbroken worden, indien naast een van de zes rechtsgronden sprake is van een wettelijke uitzonderingsgrond die het toestaat dat deze gegevens voor dit doel kunnen worden verwerkt.

14.1 Medewerkers

Xedule is een roosteringsapplicatie die ten doel heeft om het onderwijs te organiseren op basis van de inzet en beschikbaarheid van medewerkers, faculteiten en faciliteiten. Voor het ondersteunen van de Onderwijsplanning (specifiek: Inzet- en Middelenplanning) kan de reden van afwezigheid van medewerkers in Xedule en My Xedule worden verwerkt, waaronder zwangerschap of ziekte. Deze persoonsgegevens kunnen handmatig worden ingevoerd door de medewerker zelf of door de roosteraar. Het is ook mogelijk om deze gegevens automatisch te importeren. Zwangerschap en ziekte (waaronder bedrijfsongevallen) zijn gegevens over gezondheid en daarmee bijzondere persoonsgegevens.

Er is een uitzonderingsgrond van toepassing, namelijk artikel 9 lid 2 sub b AVG (verplichtingen en rechten arbeidsrecht, sociaal zekerheidsrecht en sociaal beschermingsrecht) in combinatie met artikel 30 lid 1 UAVG. Werkgevers mogen gezondheidsgegevens verwerken voor “een goede uitvoering van wettelijke voorschriften, pensioenregelingen of collectieve arbeidsovereenkomsten die voorzien in aanspraken die afhankelijk zijn van de gezondheidstoestand van de betrokkene”. Werkgevers mogen onder andere registreren dat een werknemer ziek is en of de ziekte verband houdt met een arbeidsongeval.³⁸ Ook mogen werkgevers zwangerschapsverlof registreren voor zover noodzakelijk om te kunnen voldoen aan de verlofverplichtingen van de Wet arbeid en zorg.

14.2 Studenten

Voor studenten met bepaalde fysieke of mentale beperkingen of behoeften kunnen specifieke voorzieningen en/of hulpmiddelen worden ingezet. Met deze studenten worden individuele afspraken gemaakt om ervoor te zorgen dat zij tijdens tentamens of examens over de benodigde hulpmiddelen beschikken. Deze voorzieningen worden handmatig

³⁸ Regels voor werkgevers bij zieke werknemers | Autoriteit Persoonsgegevens, geraadpleegd op 25 april 2025.

ingevoerd in Xedule, zodat ze op het juiste moment (bijvoorbeeld een examen) beschikbaar zijn. De toekenning van deze hulpmiddelen wordt ingevoerd door de roosteraar of daartoe aangewezen personen op basis van een picklist die wordt beheerd door de onderwijsinstelling. Aangezien de persoonsgegevens, die in dit kader in Xedule worden verwerkt, duiden op een beperking of gezondheidsstatus, zijn het gegevens over gezondheid en geldt in beginsel een verwerkingsverbod.

De uitzonderingsgrond die van toepassing is, is artikel 9, lid 2, onder g (Noodzaak algemeen belang) in combinatie met artikel 30 lid 1 sub a UAVG. Instellingen hebben op basis van de Wet gelijke behandeling op grond van handicap of chronische ziekte de plicht om toegankelijk onderwijs aan te bieden. Dat betekent in dit kader dat ze redelijke aanpassingen tijdens examens en toetsen moeten bieden. De verwerking van bijzondere persoonsgegevens, zoals welke hulpmiddelen een student nodig heeft, in Xedule is noodzakelijk om deze specifieke examens en toetsen te kunnen faciliteren.

Conclusie Er zijn dus uitzonderingsgronden beschikbaar voor de verwerking van bijzondere persoonsgegevens van studenten in bovenstaande situaties. Het is aan instellingen om te beoordelen of ze voldoen aan de AVG-voorwaarden om een geslaagd beroep te kunnen doen op deze uitzonderingsgronden voor het verwerken van de bijzondere persoonsgegevens in Xedule.

15 Doelbinding

Het doelbindingsbeginsel schrijft volgens artikel 5 lid 1 sub b AVG het volgende voor:

“Persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt”. Instellingen moet volgens artikel 5 lid 2 AVG kunnen aantonen dat ze voldoen aan dit beginsel.

15.1 Interne doelbinding

De persoonsgegevens van medewerkers en studenten zijn primair verzameld in het HR-systeem en het SIS met als oorspronkelijke doel om personeels- en studentenadministratie te beheren. Binnen het kader van Onderwijsplanning (roostering en planningsdoelen) worden deze persoonsgegevens vervolgens secundair verwerkt in Xedule en My Xedule. Deze verwerking is in lijn met het oorspronkelijke doel, daar het correct roosteren van studenten en medewerkers essentieel is voor de uitvoering van het onderwijsproces.

Conform artikel 6 lid 4 AVG is beoordeeld of het secundaire gebruik van de persoonsgegevens verenigbaar is met het oorspronkelijke doel. Daarbij is gekeken naar (i) het verband tussen het oorspronkelijke doel en het nieuwe doel; (ii) de context waarin de persoonsgegevens worden verzameld (wat is de relatie tussen de verwerkingsverantwoordelijke en de betrokkene?); (iii) de soort en aard van de persoonsgegevens (gaat het om gevoelige of bijzondere persoonsgegevens?); (iv) de mogelijke gevolgen van de verdere verwerking (wat zijn de gevolgen voor de betrokkene?) en (v) de passende waarborgen voor de gegevensverwerking (bv. versleuteling van persoonsgegevens). De verdere verwerking voor roosterdoeleinden staat nauw in verband met het oorspronkelijke doel van onderwijs- en personeelsadministratie en valt daarmee binnen de redelijke verwachting van studenten en medewerkers. De gegevens zijn in beginsel doorgaans niet van gevoelige aard, er is geen sprake van verdere verwerking met aanzienlijke impact op de rechten en vrijheden van de betrokkenen en passende maatregelen zijn getroffen. Gesteld kan worden dat de verdere verwerking verenigbaar is met het oorspronkelijke doel. Het is dus mogelijk voor instellingen om aan te tonen dat ze voor hun interne verwerkingen voldoen aan het doelbindingsbeginsel.

15.2 Doelbinding Xedule

In hoofdstuk 13.2 is al uitgewerkt dat de verdere verwerkingen die Xedule uitvoert met de persoonsgegevens die het bedrijf via de instellingen heeft verkregen niet verenigbaar zijn met de originele doelen. Daarom kunnen instellingen zolang die verwerkingen plaatsvinden niet aantonen dat ze voldoen aan het doelbindingsbeginsel.

16 Noodzaak en evenredigheid

De AVG geeft in artikel 5 lid 1 sub c als beginsel dat de gegevensverwerking wordt beperkt tot wat noodzakelijk is voor de verwerkingsdoeleinden. Dit beginsel van minimale gegevensverwerking/dataminimalisatie komt verder tot uitdrukking door het gebruik van het woord ‘noodzakelijk’ in artikel 6 AVG. De AVG eist hiermee dat de gegevensverwerking noodzakelijk is voor het verwezenlijken van de doeleinden. De gegevensverwerking moet daarbij de toets aan de beginselen van proportionaliteit en subsidiariteit kunnen doorstaan.

Proportionaliteit (evenredigheid) betekent dat moet worden beoordeeld of de inbreuk van de gegevensverwerking in een redelijke verhouding staat tot het doel. Bij subsidiariteit (noodzakelijkheid) wordt bekeken of de verwerkingsdoeleinden met minder ingrijpende middelen kunnen worden bereikt.

Ter beoordeling van de proportionaliteit kunnen de volgende vragen worden gesteld:

- Staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?
- Is de gegevensverwerking van persoonsgegevens te verwachten en voorzienbaar voor de betrokkenen?
- Hoe groot is het belang om de verwerkingsdoeleinden te bewerkstelligen?
- Is de gegevensverwerking het meest effectieve middel om het doeleinde te bereiken?

16.1 Subsidiariteit

Een alternatief voor het centrale rooster- en planningsproces in Xedule zou zijn om dit op decentraal niveau (groeps- of faculteitsniveau) te doen. Dit beperkt weliswaar de omvang van de te verwerken persoonsgegevens, maar heeft als nadeel een overkoepelend overzicht bemoeilijk wordt en afstemming tussen afdelingen hierdoor minder efficiënt wordt. Een ander alternatief is om andere rooster- en planningsapplicatie te gebruiken. Deze DPIA heeft geen marktonderzoek gedaan naar alternatieve applicaties. Of er een minder ingrijpend alternatief beschikbaar is zal dus per instelling afhangen van de andere applicaties die – mogelijk via aanbestedingen – beschikbaar zijn. Instellingen zullen een afweging moeten maken of deze alternatieve applicaties het mogelijk voor ze maken om hun doelen te bereiken op een minder ingrijpende manier voor betrokkenen, doordat de applicaties fundamenteel anders zijn ingericht.

16.2 Proportionaliteit

Om de proportionaliteit van de verwerkingen in Xedule en My Xedule te beoordelen moet er voldoende inzicht zijn in de manier waarop persoonsgegevens verwerkt worden, welke waarborgen er zijn voor de privacy van betrokkenen en of die voldoende zijn om de verwerkingen proportioneel te maken in verhouding tot de nagestreefde doeleinden.

Onderwijsplanning en roostering

De betrokkenen mogen en kunnen redelijkerwijs verwachten dat hun persoonsgegevens worden gebruikt voor roostering en planning. Zonder de verwerking van persoonsgegevens uit het HR-systeem en studentinformatiesysteem (SIS) is het niet mogelijk om roosters en planningen correct op te stellen en medewerkers en studenten in te delen. Daarmee is een goede onderwijsplanning essentieel voor de studievoortgang, onderwijskwaliteit en effectieve inzet van personeel en hebben instellingen dus een redelijk belang bij de verwerkingen. Aan de andere kant speelt het privacybelang van de betrokkenen. Om de verwerkingen proportioneel te maken, zijn er aan de ene kant maatregelen die instellingen zelf kunnen treffen. Het is bijvoorbeeld aan hen om de juiste autorisaties in te stellen, Xedule instructies te geven voor de benodigde applicatielogging, bewaartermijnen te hanteren en niet meer persoonsgegevens te importeren in de applicaties dan noodzakelijk is voor hun processen. Ook kunnen instellingen zelf de pick lists beheren waarmee roosterbeschikbaarheid en afwezigheid mee worden doorgegeven en instructies geven aan gebruikers om te voorkomen dat er meer bijzondere persoonsgegevens in de applicaties worden verwerkt dan noodzakelijk.

Aan de andere kant heeft Xedule een rol in het faciliteren van proportionele verwerkingen. Waarborgen die momenteel missen zijn:

1. Geen onderscheid kunnen maken tussen de gegevens waar gebruikers toegang toe krijgen door middel van de Xedule Rest API.
2. Geautomatiseerde bewaartermijnen mogelijk maken in de applicaties.
3. Het loskoppelen van de motivatie bij beschikbaarheden wanneer een leidinggevende de beschikbaarheid van werknemers doorstuurt naar de roosteraar.

Andere waarborgen waar Xedule meer bij zou kunnen ondersteunen zijn:

4. Geen velden voor persoonsgegevens aanbieden die niet noodzakelijk zijn voor de hoofddoelen waarvoor Xedule en My Xedule worden aangeboden.³⁹

³⁹ Instellingen kunnen hier zelf al per veld bepalen of deze (on)zichtbaar en/of (on)bewerkbaar zijn voor specifieke gebruikers of rollen. Het is dus mogelijk om velden voor geen enkele gebruiker of rol zichtbaar te maken.

5. Pseudonimisering toepassen wanneer de identiteit van gebruikers niet noodzakelijk is voor de verwerkingen in de applicaties, bijvoorbeeld door logginggegevens niet te koppelen aan namen van gebruikers.

Instellingen moeten dus in ieder geval de beschreven stappen nemen om tot proportionele verwerkingen in Xedule en My Xedule te komen, maar zonder het toepassen van de eerste drie maatregelen door Xedule kunnen de verwerkingen in de beide applicaties niet proportioneel zijn.

Overige doeleinden Xedule

Zoals beschreven in 8.3 is er weinig transparantie over de verwerking van zowel contentdata, diagnostische data en accountdata die Xedule verwerkt voor haar eigen doeleinden. Zonder meer inzicht in deze verwerkingen kan er niet geconcludeerd worden dat de verwerkingen hiervoor proportioneel zijn.

17 Rechten van de betrokkenen

Medewerkers en studenten moeten de mogelijkheid hebben om hun wettelijke rechten te kunnen uitoefenen op de persoonsgegevens die in Xedule en My Xedule worden verwerkt. De onderwijsinstelling is als verwerkingsverantwoordelijke gehouden om dergelijke verzoeken te honoreren en Xedule dient te faciliteren. Dit betekent dat door Xedule in opdracht van de onderwijsinstelling binnen één maand na ontvangst van een verzoek van betrokkene hiertoe onder andere inzage moet verschaffen in de persoonsgegevens die verwerkt worden, rectificeren of wissen van persoonsgegevens en of tijdelijk beperken. Voor de verwerkingen waar Xedule zelf verantwoordelijk is, is Xedule ook verantwoordelijk voor het beantwoorden van inzageverzoeken.

Daarbij moet er voorafgaand aan de verwerking informatie worden verstrekt over de te verwerken persoonsgegevens (informatieplicht) en hebben de betrokkenen het recht om een klacht in te dienen bij de AP.

Wettelijk recht	Onderwijsinstelling	Xedule
Recht op inzage	Voor accountdata en contentdata kan onderwijsinstelling volledige inzage geven. Instellingen kunnen volledige inzage geven in accountdata en contentdata.	Xedule heeft onvoldoende inzage in diagnostische data in systeemlogging gegeven.
Recht op rectificatie	Persoonsgegevens in Xedule zijn afkomstig uit bronsystemen en kunnen enkel in de bronsystemen gewijzigd worden. Contentdata kan worden aangepast wanneer hier overeenstemming over is tussen onderwijsinstelling en betrokkene.	Diagnostische data worden bewaard zoals ze worden uitgelezen, hier zijn geen aanpassingen op van toepassing.
Recht op wissing	Accountdata en contentdata kunnen worden verwijderd wanneer hier overeenstemming over is tussen onderwijsinstelling en betrokkene.	SURF heeft dit niet kunnen toetsen.

Recht op beperking	Accountdata en contentdata kunnen worden beperkt wanneer hier overeenstemming over is tussen onderwijsinstelling en betrokkene.	SURF heeft dit niet kunnen toetsen.
Recht van bezwaar		SURF heeft dit niet kunnen toetsen.

C. Beschrijving en beoordeling risico's voor betrokkenen

18 Risico's voor betrokkenen

Inleiding

Deel C bevat de risicoanalyse van de huidige risico's, waarin de gegevensverwerkingsanalyse (Deel A) en de beoordeling van de rechtmatigheid (Deel B) worden besproken. Deze beoordeling wordt afgezet tegen de rechten en vrijheden van betrokkenen. Daarbij worden de risico's van de voorgenomen gegevensverwerkingen geëvalueerd, rekening houdend met de aard, omvang, context en doelen van de verwerkingen. In deze analyse zijn de te treffen maatregelen van onderdeel D nog niet meegenomen.

Beoordelingskader risico's

Bij de beoordeling van de gegevensverwerkingen wordt gekeken naar de mogelijke risico's voor de rechten en vrijheden van betrokkenen. Hierbij wordt gekeken naar:

- De mogelijke negatieve gevolgen van de verwerking.
- De oorsprong van de gevolgen.
- De kans (waarschijnlijkheid) dat deze gevolgen zich voordoen.
- De ernst (impact) van de gevolgen.

De risicoanalyse volgt de methodiek die is beschreven door de Britse toezichthouder (ICO) om risico's te classificeren.⁴⁰ Hierbij wordt een objectieve inschatting gemaakt van de kans (waarschijnlijkheid) en impact (ernst) van mogelijke negatieve gevolgen, zoals fysieke, emotionele of materiële schade.⁴¹ De kans dat de schade optreedt gecombineerd met de impact van die schade is het resulterende risico.

Classificatie van risico's

Om de factoren kans en impact visueel weer te geven en te classificeren wordt gebruik gemaakt van een risicomatrix.

⁴⁰ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/>, geraadpleegd op 2 mei 2025.

⁴¹ <https://ico.org.uk/media2/about-the-ico/documents/4020144/overview-of-data-protection-harms-and-the-ico-taxonomy-v1-202204.pdf>, geraadpleegd op 12 juni 2025.

Impact van de schade	Zware impact	Laag risico	Hoog risico	Hoog risico
	Enige impact	Laag risico	Medium risico	Hoog risico
	Minimale impact	Laag risico	Laag risico	Laag risico
		Lage kans	Redelijke kans	Waarschijnlijk
	Kans dat er schade plaatsvindt			

18.1 Verlies van controle door Xedule als verwerkingsverantwoordelijke

Xedule kwalificeert als feitelijke verwerkingsverantwoordelijke voor een aantal verwerkingen, zoals beschreven in paragraaf 8.3. Doordat Xedule deze rol heeft kunnen de instellingen geen instructies geven over de gegevensverwerkingen die Xedule uitvoert met de gegevens van studenten en medewerkers die de instellingen aan Xedule verstrekken. Hierdoor is het voor de instellingen niet mogelijk om de veilige, rechtmatige verwerking van de persoonsgegevens van betrokkenen van de instellingen te waarborgen.

De waarschijnlijkheid dat dit zich voordoet is 100%, want de juridische en feitelijke werkelijkheid is dat Xedule verantwoordelijk is voor de beschreven verwerkingen. De impact is hoog, omdat dit invloed heeft op alle systeemlogginggegevens (onder andere over het gedrag van gebruikers), gegevens in de applicatie en gebruikersfeedback die Xedule verwerkt van kwetsbare betrokkenen. Gegevens kunnen voor andere doeleinden verwerkt worden en aan derden worden verstrekt.

18.2 Verlies van controle door gebrek aan transparantie logging, pNPS en marketing

Xedule voert systeemlogging uit als verwerkingsverantwoordelijke ten behoeve van de doelen verbetering van de applicatie en fraudepreventie en beveiliging. De gelogde gegevens worden gekoppeld aan de namen van de gebruikers en zijn dus persoonsgegevens. Xedule geeft echter geen volledig overzicht van de 'items' die worden gelogd en biedt hier ook geen inzage in bij de inzageverzoeken of het technisch onderzoek. Er wordt enkel op hoofdlijnen beschreven welke soorten logging plaatsvinden en wat het algemene doel van elk type logging is. De feitelijk gelogde gegevens zijn slechts op hoog niveau gecategoriseerd, waardoor het moeilijk is om de proportionaliteit van de logging te beoordelen (worden de gegevens bijvoorbeeld op enig punt in het proces gepseudonimiseerd of geanonimiseerd?). Daarnaast is de toegang tot de logs slechts summier beschreven, zonder duidelijke vermelding van autorisatieprocedures of toegangsbeperkingen. Ook voert Xedule pNPS-verwerkingen uit voor dienstverbetering, inclusief pseudonisering en verwerking in een 'big data oplossing' en verwerkingen voor marketing, waar weinig over bekend is.

Dit gebrek aan transparantie leidt ertoe dat het voor gebruikers niet duidelijk is waar hun gegevens mogelijk voor worden gebruikt. Het is niet mogelijk te beoordelen of de logging rechtmatig is, proportioneel is en wie wanneer toegang heeft tot de loggegevens. Dit kan leiden tot situaties waarin ongeautoriseerde en ongecontroleerde toegang tot (gevoelige) gegevens onopgemerkt blijft. Het risico bestaat dat de gegevens voor doeleinden worden gebruikt die niet verenigbaar zijn met de originele doelen, wat een verlies van controle, vertrouwelijkheid en psychische stress kan opleveren.

De kans dat deze gevolgen zich voordoen zijn 100%, omdat er door het gebrek aan transparantie helemaal geen controle over deze gegevens is. De impact is ook groot, omdat het om veel gegevens en om bijzondere persoonsgegevens gaat.

18.3 Verlies van vertrouwelijkheid en sociaal nadeel door te brede definiëring afwezigheids- en hulpmiddelencategorieën

Het is voor zowel de betrokkene zelf als de roosteraar mogelijk om in pick lists en open velden de reden van afwezigheid te registreren bij roosterconflicten, waaronder ziekte en zwangerschap. Ook kunnen instellingen door middel van zelf te definiëren categorieën bijhouden welk type verlof medewerkers hebben en op welke hulpmiddelen studenten recht hebben. Er bestaat een risico dat de pick lists verkeerd worden gedefinieerd, waardoor instellingen gegevens verwerken waarvoor ze geen grondslag of uitzonderingsgrond hebben. Dit kan er voor betrokkenen tot leiden dat ze anders behandeld worden op basis van hun gezondheidsgegevens en dat de vertrouwelijkheid van hun gezondheidsgegevens in het geding komt.

De kans dat dit gebeurt is redelijk als er geen duidelijk beleid is, aangezien de invulling dan afhankelijk is van individuele inschattingen van functionele medewerkers. De impact is zwaar, omdat er sprake is van bijzondere persoonsgegevens.

18.4 Niet mogelijk om AVG-rechten uit te oefenen en verlies van controle door gebrek aan transparantie subverwerkers

Hoewel Xedule is reeds actief bezig is met het herzien en aanvullen van het overzicht van de subverwerkers en het aanscherpen van de subverwerkersovereenkomsten, bleek op het moment van onderzoek uit de documentatie van Xedule niet duidelijk aan welke partijen de subverwerkers persoonsgegevens verstrekken en om welke persoonsgegevens dit zou gaan. Dit maakt het voor de instellingen als verwerkingsverantwoordelijken moeilijk om het benodigde inzicht in de ontvangende partijen te verkrijgen en te verstrekken aan betrokkenen. Voor betrokkenen heeft dit het gevolg dat ze hun recht op inzage moeilijker kunnen uitoefenen, doordat een overzicht van ontvangers mogelijk niet (tijdig) beschikbaar is. Daarnaast kunnen de gegevens van betrokkenen hierdoor verwerkt worden door partijen

waar geen controle op is, waardoor hun gegevens voor andere doeleinden gebruikt kunnen worden en er een verlies van vertrouwelijkheid kan optreden.

De waarschijnlijkheid dat dit risico optreedt is 100%, aangezien er momenteel geen overzicht is van de subverwerkers van Xedule. De impact is hoog, omdat het gaat om alle gegevens die in Xedule en My Xedule verwerkt worden onder dit risico vallen, waaronder bijzondere persoonsgegevens. Daarnaast is het uitoefenen van AVG-rechten een fundamenteel recht van betrokkenen. Het niet kunnen uitoefenen hiervan heeft dus een grote impact.

18.5 Verlies van vertrouwelijkheid door doorgeven beschikbaarheidsredenen aan roosteraars

Docenten kunnen hun beschikbaarheidsopgave via My Xedule voorzien van motivatie via een vrij veld. Deze motivatie dient als verduidelijking van het wel of niet beschikbaar zijn op dat dagdeel. Na goedkeuring door leidinggevendenden van deze beschikbaarheidsopgaven worden deze inclusief persoonlijke motivaties automatisch doorgestuurd naar roosteraars. Leidinggevendenden hebben legitieme redenen om toegang te hebben tot de motivaties van docenten voor hun beschikbaarheid, aangezien dit relevant is voor het beoordelen van verzoeken. Roosteraars daarentegen hebben deze persoonlijke informatie niet nodig om hun taken effectief uit te voeren. Het verstrekken van deze gegevens aan roosteraars is daarom niet proportioneel, maar het is technisch niet mogelijk om de motivaties los te koppelen voor het doorsturen naar de roosteraars. Daarbij moet worden opgemerkt dat de kans aannemelijk is dat er gevoelige en bijzondere persoonsgegevens worden gedeeld via deze schriftelijke motivatie. Er bestaat dus een risico op verlies van vertrouwelijkheid.

De kans dat dit risico zich voordoet is 100% aangezien dit standaard in een kernproces van de applicaties plaatsvindt. Er is enige impact, aangezien de kans groot is dat er gevoelige en zelfs bijzondere gegevens gedeeld worden bij het 'goedkeurings'proces rond beschikbaarheid, maar de gegevens worden met een beperkte groep roosteraars gedeeld die onder dezelfde organisatie vallen als de leidinggevende.

18.6 Verlies van controle en vertrouwelijkheid door overige vrije velden

Het is mogelijk om door middel van vrij in te vullen velden opmerkingen toe te voegen aan dossiergegevens van personen. Deze vrije velden dienen geen bepaald doel en instellingen zijn dus vrij hier zelf invulling aan te geven. Ook kunnen studenten een motivatie toevoegen in een vrij veld bij inschrijvingen. Er is een waarschuwing in het openingsscherm van de gebruiker dat het niet de bedoeling is om deze vrije velden te gebruiken voor bijzondere persoonsgegevens, met een link naar meer informatie. Deze link leidt tot een foutmelding in de testomgeving en zou in de productieomgeving naar de privacyverklaring moeten leiden. Het bestaan van deze vrije velden leidt tot het risico dat gebruikers hier persoonsgegevens

in registreren waarvoor instellingen geen verwerkingsgrondslag en uitzonderingsgrond voor bijzondere persoonsgegevens hebben. Dit kan leiden tot een verlies van controle over de gegevens, doordat de gegevens bijvoorbeeld te lang bewaard worden en tot een verlies van vertrouwelijkheid.

Ervan uitgaande dat er verder geen sturing is vanuit de instellingen om bovenstaande te voorkomen, is de kans dat dit gebeurt is redelijk, omdat dit risico afhankelijk is van menselijke feilbaarheid, een bekende oorzaak van privacy- en securityincidenten. De eenmalige melding om geen bijzondere persoonsgegevens in te vullen in de velden met een kapotte link doet hier niet aan af. De impact is zwaar, omdat er bijzondere persoonsgegevens bij betrokken kunnen zijn.

18.7 Gemiste kansen en verlies van vertrouwelijkheid door handmatige invoer

Roosteraars en/of functioneel beheerders kunnen handmatig persoonsgegevens invoeren en bewerken in Xedule. Deze handmatige verwerking vindt plaats via directe invoer in het systeem, waarbij nieuwe persoonsgegevens kunnen worden toegevoegd en bestaande gegevens kunnen worden gewijzigd of verrijkt. Denk hierbij aan het handmatig doorvoeren van roosterwijzigingen, verlof en het aanpassen van gebruikersgegevens. Er zijn in Xedule en My Xedule geen standaard controles bij invoer waardoor mogelijk onjuiste gegevens of (bijzondere of gevoelige) persoonsgegevens zonder grondslag ongecontroleerd worden verwerkt. Dit kan bijvoorbeeld leiden tot het delen van informatie met de verkeerde personen, gemiste lessen en het ontbreken van het recht niet toegekend krijgen van verlof. Daarnaast kunnen er hierdoor discrepanties ontstaan met de gegevens in de bronsystemen?

De kans dat deze gevolgen optreden is redelijk, omdat dit risico afhankelijk is van menselijke feilbaarheid en er momenteel geen maatregelen zijn om de gevolgen te voorkomen. De gevolgen zijn direct merkbaar in het leven van betrokkenen en hebben daarmee enige impact.

18.8 Verlies van controle en vertrouwelijkheid door niet automatisch te configureren bewaartermijnen

Xedule en My Xedule bieden geen functionaliteit aan die het mogelijk maakt om persoonsgegevens na het verstrijken van de bewaartermijn geautomatiseerd te verwijderen of om een melding te krijgen na het verstrijken van een bewaartermijn. Daarnaast is het niet mogelijk om onderscheid te maken tussen categorieën persoonsgegevens waar verschillende bewaartermijnen voor kunnen gelden. Dit leidt tot het risico voor betrokkenen dat hun persoonsgegevens langer worden bewaard dan noodzakelijk. Dit kan leiden tot een verlies van controle doordat gegevens langer bewaard worden dan rechtmatig is en tot verlies van vertrouwelijkheid.

De kans dat dit risico zich realiseert is groot, omdat het momenteel erg moeilijk is voor instellingen een effectief bewaartermijnenbeleid te implementeren in Xedule en My Xedule. De impact is groot, doordat dit risico alle persoonsgegevens in Xedule en My Xedule raakt, waaronder de bijzondere persoonsgegevens.

18.9 Niet uit kunnen oefenen van AVG-rechten door incomplete inzageverzoeken

Xedule heeft als reactie op het inzageverzoek instructies verstrekt voor het ophalen van gegevens die inzichtelijk zijn voor beheerders van Xedule, maar heeft geen informatie verstrekt over logging en verwerkingen van diagnostische gegevens. Deze logging en diagnostische gegevens zijn niet inzichtelijk voor beheerders vanuit instellingen en betrokkenen zijn dus afhankelijk van Xedule. SURF heeft tijdens het inzageverzoek van meerdere gebruikers de persoonsgegevens opgevraagd. Bij deze verzoeken heeft SURF als bijlage meerdere identificatieparameters aangeleverd. Xedule heeft ruim na de reactietermijn een incompleet inzageverzoek van één gebruiker aangeleverd naar aanleiding van onze verzoeken. Het niet volledig voldoen aan inzageverzoeken maakt dat betrokkenen hun rechten niet kunnen uitoefenen en geen volledig inzicht hebben in welke gegevens over hen worden verwerkt en hoe deze worden gebruikt.

De kans dat betrokkenen hun inzagerecht (en andere AVG-rechten) niet kunnen uitoefenen is waarschijnlijk, aangezien Xedule niet in staat was voor slechts zes betrokkenen tijdige en complete inzage te bieden. De impact hiervan is zwaar, omdat het kunnen uitoefenen van het inzagerecht noodzakelijk is om andere AVG-rechten te kunnen uitoefenen. Al deze rechten zijn fundamentele rechten van betrokkenen.

18.10 Verlies van controle en vertrouwelijkheid door het niet hebben van automatische import/export

Het handmatig importeren en exporteren van stamgegevens uit bronsystemen brengt risico's met zich mee voor de integriteit van persoonsgegevens. Deze methode is vatbaar voor menselijke fouten, zoals het per ongeluk importeren van onjuiste of verouderde gegevens, wat kan leiden tot onjuiste verwerkingen. Deze handmatige aanpak vergroot ook het risico op ongeautoriseerde toegang tot gevoelige informatie. Geautoriseerde medewerkers die de import/export uitvoeren, hebben potentieel toegang tot meer gegevens dan strikt noodzakelijk voor hun functie, wat in strijd is met het principe van minimale gegevensverwerking uit de AVG. Deze handmatige aanpak verhoogt ook het risico op datalekken, aangezien geëxporteerde bestanden gemakkelijk gedeeld of opgeslagen kunnen worden op onbeveiligde locaties. Er is dus een risico op verlies van controle en vertrouwelijkheid van de gegevens.

De kans dat de controle over en de vertrouwelijkheid van de gegevens verloren wordt is redelijk, aangezien er door de handmatige invoer rekening gehouden moet worden met menselijke feilbaarheid. Omdat de stamgegevens uit de bronsystemen gevoelige gegevens, zoals locatiegegevens kunnen bevatten, is de impact van deze gevolgen groot.

18.11 Verlies van controle en vertrouwelijkheid door tabellen

Het veelvuldig gebruik van tabellen in de interface, hoewel gebruiksvriendelijk, vormt een risico voor de bescherming van persoonsgegevens. Alle gebruikers die toegang hebben tot de tabellen kunnen gemakkelijk persoonsgegevens uit deze tabellen kopiëren en exporteren uit naar andere systemen. Dit kan resulteren in ongecontroleerde verspreiding en het ontstaan van schaduwadministraties, wat haaks staat op het principe van Privacy by Design. Er is dus een risico op verlies van controle en vertrouwelijkheid van de gegevens in de tabellen, door het exporteren van de gegevens naar andere systemen en andere leveranciers. De bewaartermijnen van de gegevens kunnen ook overschreden worden als ze bewaard worden in andere systemen,

Ervan uitgaande dat er geen instructies zijn voor het gebruik van de tabellen is de kans dat bovenstaande gebeurt redelijk, omdat gebruikers dan niet weten dat ze gegevens niet mogen exporteren. De impact is ook groot, omdat de tabellen ook bijzondere persoonsgegevens kunnen bevatten.

18.12 Verlies van vertrouwelijkheid door handmatige RBAC

Het alleen handmatig kunnen toekennen van gebruikersrollen en rechten in Xedule brengt risico's met zich mee voor de beveiliging en privacy van persoonsgegevens. Hoewel de aanwezigheid van standaardrollen gebaseerd op best practices een goede basis biedt, introduceert de mogelijkheid voor beheerders om rollen aan te maken, te wijzigen en te specificeren kwetsbaarheden. De afwezigheid van een geautomatiseerde koppeling met externe identiteits- en toegangsbeheersystemen vergroot de kans op menselijke fouten bij het toewijzen van rechten. Dit kan leiden tot situaties waarin gebruikers te veel of te weinig rechten krijgen, waarbij het risico op verlies van vertrouwelijkheid van gegevens ontstaat.

De kans dat de vertrouwelijkheid van de gegevens verloren wordt is redelijk, aangezien er door de handmatige invoer rekening gehouden moet worden met menselijke feilbaarheid. De impact kan hoog zijn, aangezien er bijzondere persoonsgegevens in Xedule en My Xedule worden verwerkt.

18.13 Verlies van vertrouwelijkheid door onduidelijke configuratiewijzigingen

Functioneel beheerders kunnen instellingen wijzigen die directe invloed hebben op de autorisatiestructuur van zowel Xedule als My Xedule, zonder dat de interface zelf duidelijk maakt wat de impact van deze wijzigingen is. Dit gebrek aan transparantie in de interface

vergroot het risico op fouten in autorisaties. De noodzaak om handleidingen te raadplegen voor het begrijpen van de impact van instellingswijzigingen is een argument dat de interface zelf tekortschiet in het bieden van essentiële informatie. Het is mogelijk dat er autorisatiewijzigingen plaatsvinden zonder dat gebruikers dat doorhebben, wat leidt tot een risico op verlies van vertrouwelijkheid.

De kans op verlies van vertrouwelijkheid is redelijk, omdat er rekening gehouden moet worden met menselijke feilbaarheid en er in de interface geen indicatie is dat er (foute) wijzigingen zijn doorgevoerd. De impact kan hoog zijn, aangezien er bijzondere persoonsgegevens in Xedule en My Xedule worden verwerkt.

18.14 Verlies van vertrouwelijkheid door Xedule rest API

Het huidige autorisatiemodel van de Xedule API zorgt dat de koppeling toegang biedt tot alle gegevens binnen Xedule, zonder de mogelijkheid om te bepalen welke gegevenssets nodig zijn voor het doel waar de koppeling voor gebruikt wordt. Dit kan leiden tot overmatige gegevensblootstelling, aangezien de API-koppeling externe systemen toegang geeft tot meer gegevens dan noodzakelijk voor het doel. Aangezien toegang door middel van de API niet beperkt is tot specifieke datasets of functies, leidt dit tot het risico van verlies van vertrouwelijkheid van gegevens.

De kans dat dit verlies van vertrouwelijkheid optreedt is afhankelijk van externe systemen waar Xedule geen controle over heeft en moet dus worden ingeschat op waarschijnlijk. De impact kan hoog zijn, aangezien er bijzondere persoonsgegevens in Xedule en My Xedule worden verwerkt.

18.15 Verlies van vertrouwelijkheid en controle door ongeautoriseerde toegang door verouderde SOAP API

Het gebruik van de verouderde SOAP API brengt risico's met zich mee. Hoewel Xedule aangeeft dat de beveiliging nog wordt onderhouden is het riskant om afhankelijk te zijn van een technologie die niet meer actief wordt ontwikkeld. Dit kan leiden tot een risico op ongeautoriseerde toegang tot persoonsgegevens.

Aangezien er naast het autorisatiemodel van de API ook RBAC-autorisatie in de applicatie plaatsvindt, is de kans dat er onterechte toegang tot gegevens plaatsvindt redelijk. De impact kan hoog zijn, aangezien er bijzondere persoonsgegevens in Xedule en My Xedule worden verwerkt.

18.16 Heridentificering van gepseudonimiseerde gegevens door gebrekkige anonimiseringsmethode

Xedule biedt anonimisering van datasets aan als dienst. Anonimisering door enkel directe identificatoren zoals naam, e-mail en gebruikersnaam te verwijderen of vervangen voldoet niet aan de strikte AVG-vereisten voor anonimisering. Anonimisering vereist dat gegevens onomkeerbaar zijn ontdaan van alle elementen die herleiding naar individuen mogelijk maken, zowel directe als indirecte identificerende kenmerken. De grootte van de dataset is van invloed op de herleidbaarheid van de betrokkene. Met individuele studieroutes, het gebruik van vrije velden en verwerken van verloffgegevens zijn er te veel identificatoren om van anonimisering te kunnen spreken. Er moet in dit geval dan ook gesproken worden van pseudonimisering. Omdat deze datasets behandeld worden alsof ze geanonimiseerd zijn en er dus geen AVG-vereisten of andere waarborgen meer van toepassing zijn, bestaat het risico dat de gepseudonimiseerde betrokkenen opnieuw geïdentificeerd worden. Deze gegevens kunnen vervolgens voor onbedoelde doeleinden gebruikt worden of inzichtelijk worden voor ongeautoriseerde personen.

Deze verwerking vindt op aanvraag plaats, dus niet standaard. Als hij plaatsvindt, dan is de kans dat de gevolgen optreden wel groot, aangezien instellingen de gegevens behandelen als anoniem en dus geen waarborgen meer toepassen. De kans in zijn totaliteit is dus redelijk. De impact is zwaar aangezien hier bijzondere persoonsgegevens in voor kunnen komen die potentieel herleidbaar zijn naar de betrokkene en er geen controle meer is op de gegevens na heridentificatie.

18.17 Heridentificering gepseudonimiseerde pNPS-gegevens

De gegevens die verwerkt worden om klantfeedback via pNPS te analyseren, worden volgens Xedule⁴² gepseudonimiseerd voordat deze in een big data-applicatie worden opgeslagen. Analisten van Xedule hebben toegang tot deze gepseudonimiseerde gegevens. Volgens Xedule⁴³ is het in de huidige inrichting voor één individu niet mogelijk om de gegevens te herleiden tot een natuurlijk persoon, omdat daarvoor toegang tot zowel de originele als de gepseudonimiseerde data nodig is, en deze toegang is verdeeld over meerdere medewerkers. Xedule heeft hierover geen aanvullende documentatie overlegd. Dit betekent dat het niet volledig kan worden vastgesteld of de deze maatregelen zijn geïmplementeerd zoals beschreven. Daarnaast vinden deze verwerkingen plaats via een opt-out constructie. Ze vinden dus standaard plaats, tenzij de instellingen of gebruikers hier bezwaar tegen hebben. Bij onvoldoende maatregelen rondom pseudonimisering bestaat het risico op heridentificering van betrokkenen.

De kans dat deze gevolgen optreden moet hoog worden ingeschat, aangezien niet inzichtelijk is welke waarborgen er bij deze verwerkingen zijn toegepast. Er is enige impact wanneer deze gevolgen optreden, aangezien er geen bijzondere of gevoelige persoonsgegevens bij betrokken zijn.

⁴² Mailwisseling met CISO van Xedule.

⁴³ Mailwisseling met CISO van Xedule.

18.18 Verlies van vertrouwelijkheid door ontbreken 'read access logging'

Het ontbreken van logging op inzage (read access logging) vergroot het risico dat niet kan worden vastgesteld of onbevoegden daadwerkelijk persoonsgegevens hebben ingezien bij een autorisatiefout of incident. Hierdoor is het bij een potentieel datalek onmogelijk om te achterhalen of en van wie persoonsgegevens zijn ingezien door onbevoegde gebruikers. Dit betekent dat instellingen geen adequate, gerichte maatregelen kunnen treffen en de vertrouwelijkheid van de gegevens in het geding komen.

De kans dat deze gevolgen optreden is 100%, omdat het ontbreken van read access logging het onmogelijk maakt om ongeautoriseerde inzage te monitoren en mitigeren. De impact is hoog aangezien er bijzondere en/of gevoelige persoonsgegevens bij betrokken kunnen zijn en de inzage door partijen binnen en buiten de organisatie kunnen plaatsvinden.

D. Beschrijving voorgenomen maatregelen

19 Maatregelen

In dit hoofdstuk worden de technische, organisatorische en juridische maatregelen beschreven die instellingen en Xedule kunnen treffen om de hiervoor beschreven risico's te mitigeren. Per risico wordt in de bovenste helft van de tabel het huidige risico beschreven en de risicoscore uit onderdeel C weergegeven. In de onderste helft van de tabel worden de maatregelen beschreven die Xedule en de instellingen kunnen treffen en wordt er een score aan het restrisico gegeven. Daarnaast zijn de acties die Xedule heeft voorgesteld om invulling te geven aan de maatregelen per risico in een afzonderlijke tabel opgenomen, samen met een tijdslijn voor de acties.

Verlies van controle door Xedule als verwerkingsverantwoordelijke						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	
18.1	Xedule als verwerkersverantwoordelijke, waardoor instellingen geen instructies over verwerkingen kunnen geven	Verlies van controle instellingen	Waarschijnlijk	Zwaar	Hoog	Huidig risico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	Restrisico
		Juridisch en feitelijk de rol van verwerker aannemen voor alle verwerkingen waarbij instellingen Xedule geen toestemming geven voor verdere verwerking als verwerkingsverantwoordelijke	Laag	Zwaar	Laag	

Voorgestelde actie(s) Xedule	Tijdslijn
Update van Privacy Statement met verwerkingen waar Xedule de Verwerkingsverantwoordelijke is met de correcte grondslag.	Gereed 30 september 2025
Update van Verwerkersovereenkomst met verwerkingen waar Xedule de Verwerker is met meer transparantie en helderheid.	Gereed 30 september 2025

Update van Register Verwerkingen (Record of Processing Activities - ROPA). ROPA is een tool waarin eenvoudig alle verwerkingen en aanverwante informatie zoals grondslagen ingevoerd kan worden.	Wordt elk kwartaal voorzien van updates rondom Processing Activities met applicaties zowel vanuit de rol Processor als de rol Controller.
--	---

Verlies van controle door gebrek aan transparantie logging, pNPS en marketing						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risico-score	Huidig risico
18.2	Gebrek aan transparantie over gegevensverwerkingen door Xedule	Verlies van controle over onder andere systeemloggingsgegevens	Waarschijnlijk	Zwaar	Hoog	Huidig risico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risico-score	
		Inzage verschaffen in alle verwerkingen bij inzageverzoeken	Minimaal	Zwaar	Laag	
		Inzicht bieden in loggingpraktijken in complete en up-to-date documentatie, bijvoorbeeld een loggingbeleid				
		Feitelijke loggingpraktijken laten aansluiten bij gedocumenteerde loggingpraktijken				
		Inzicht bieden in pNPS-verwerkingen				

Mitigerende actie Xedule	Tijdstip
Diverse documenten en statements aanpassen met overzicht welke logging er plaatsvindt.	Gereed 30 september 2025
Diverse documenten en statements aanpassen met overzicht welke persoonsgegevens verzameld worden met welk doel en grondslag.	Gereed 30 september 2025
Aanscherpen en implementeren Loggingbeleid.	Gereed 30 september 2025
Aanscherpen/Opstellen procedure voor inzageverzoeken.	Gereed - Inzageverzoeken kunnen desgewenst ingediend worden. Elk inzageverzoek zal als bron gebruikt worden om het proces verder te verfijnen/verbeteren en waar nodig het Privacy Statement en de Verwerkersovereenkomst op aan te passen.

Verlies van vertrouwelijkheid en sociaal nadeel door te brede definiëring afwezigheids- en hulpmiddelencategorieën						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risico-score	Huidig risico
18.3	Mogelijkheid tot definiëren en verwerken categorieën (bijzondere) persoonsgegevens in pick lists en open velden	Verlies van vertrouwelijkheid en sociaal nadeel voor betrokkenen	Redelijk	Zwaar	Hoog	Restrisico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risico-score	
	Duidelijk beleid op de redenen voor afwezigheid die worden geregistreerd	Duidelijke strategie implementeren om klanten en gebruikers (in de context van de verwerking) te waarschuwen categorieën niet te breed te definiëren en geen (bijzondere) persoonsgegevens in open velden op te nemen	Laag	Zwaar	Laag	
	Duidelijke training en instructie over welke gegevens wel en niet in open velden mogen worden geregistreerd					
	Monitoring van de effectiviteit van dit beleid					

Mitigerende actie Xedule	Tijdslijn
Onderzoek naar betreffende vrije invulvelden en pick lists en waar deze ongewenst doorgezet of ingezien kunnen worden door medewerkers van instellingen. Tevens de behoefte van instellingen hierin meenemen zodat hun functionele eisen rondom deze velden bekend zijn (indien instellingen geen behoeftes kenbaar maken, worden de velden naar inzicht van Xedule passend beveiligd). Uitgangspunt onderzoek: Passende beveiliging van de velden, zodanig dat de velden afgeschermd worden voor inzage van onbevoegden en/of configurabel worden gemaakt zodat de instellingen dit zelf kunnen bepalen.	Gereed 31 oktober 2025
Bewustwordingscampagne naar onderwijsinstellingen om de risico's van de vrije velden helder te maken.	Gereed 30 september 2025
Opvolgen van de onderzoeksresultaten	Gereed 31 maart 2026

Niet mogelijk om AVG-rechten uit te oefenen en verlies van controle door gebrek aan transparantie subverwerkers						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risico-score	Huidig risico
18.4	Gebrek aan transparantie subverwerkers	Niet mogelijk om AVG-rechten volledig uit te oefenen voor betrokkenen en verlies van controle instellingen	Waarschijnlijk	Zwaar	Hoog	Restrisico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risico-score	

	Periodieke controle op overzicht subverwerkers	Hoofd- en verwerkersovereenkomsten sluiten met alle subverwerkers met een duidelijke instructie over de te verwerken persoonsgegevens en een lijst met subverwerkers	Laag	Zwaar	Laag	
--	--	--	------	-------	------	--

Mitigerende actie Xedule	Tijdslijn
Verwerkersovereenkomst uitbreiden met persoonsgegevens die door subverwerkers worden behandeld	Gereed 30 september 2025
Definitief maken contracten en subverwerkersovereenkomsten met subverwerkers. Met name het contract met een subverwerker waar in de rollen omgedraaid stonden	Gereed 31 oktober 2025
Update van Register Verwerkingen (Record of Processing Activities - ROPA). ROPA is een tool waarin eenvoudig alle verwerkingen en aanverwante informatie zoals grondslagen ingevoerd kan worden.	Wordt elk kwartaal voorzien van updates rondom Processing Activities met applicaties zowel vanuit de rol Processor als de rol Controller.

Verlies van vertrouwelijkheid door doorgeven beschikbaarheidsredenen aan roosteraars						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risico-score	Huidig risico
18.5	Doorgeven beschikbaarheidsredenen aan roosteraars	Verlies van vertrouwelijkheid	Waarschijnlijk	Enige	Hoog	Huidig risico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risico-score	
	Implementeer bewaartermijnen voor de motivatie	Mogelijkheid implementeren om beschikbaarheidsredenen te verbergen voor gebruikers die er geen toegang toe nodig hebben voor hun functie	Laag	Enige	Laag	Restrisico
	Geef duidelijke instructie aan gebruikers wat er wel en niet in de open velden moet worden ingevuld	Duidelijke strategie implementeren om klanten en gebruikers (in de context van de verwerking) te waarschuwen geen				

		(bijzondere) persoonsgegevens in open velden op te nemen				
--	--	--	--	--	--	--

Mitigerende actie Xedule	Tijdslijn
Onderzoek naar betreffende vrije invulvelden en waar deze ongewenst doorgezet of ingezien kunnen worden door medewerkers van instellingen. Tevens de behoefte van instellingen hierin meenemen zodat hun functionele eisen rondom deze velden bekend zijn (indien instellingen geen behoeftes kenbaar maken, worden de velden naar inzicht van Xedule passend beveiligd). Uitgangspunt onderzoek: Passende beveiliging van de velden, zodanig dat de velden afgeschermd worden voor inzage van onbevoegden en/of configurabel worden gemaakt zodat de instellingen dit zelf kunnen bepalen.	Gereed 31 oktober 2025
Bewustwordingscampagne naar onderwijsinstellingen om de risico's van de vrije velden helder te maken.	Gereed 30 september 2025
Opvolgen van de onderzoeksresultaten	Gereed 31 maart 2026

Verlies van controle en vertrouwelijkheid door overige vrije velden						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	Huidig risico
18.6	Invullen vrije velden	Verlies van controle en vertrouwelijkheid	Redelijk	Zwaar	Hoog	Restrisico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	
	Duidelijke training en instructie over welke gegevens wel en niet in open velden mogen worden geregistreerd	Duidelijke strategie implementeren om klanten en gebruikers (in de context van de verwerking) te waarschuwen geen (bijzondere) persoonsgegevens in open velden op te nemen	Laag	Zwaar	Laag	
	Monitoring van de effectiviteit van dit beleid					

Mitigerende actie Xedule	Tijdslijn
Onderzoek naar betreffende vrije invulvelden en waar deze ongewenst doorgezet of ingezien kunnen worden door medewerkers van instellingen. Tevens de behoefte van instellingen hierin meenemen zodat hun functionele eisen rondom deze velden bekend zijn (indien instellingen geen behoeftes kenbaar maken, worden de velden naar inzicht van Xedule passend beveiligd). Uitgangspunt onderzoek: Passende	Gereed 31 oktober 2025

beveiliging van de velden, zodanig dat de velden afgeschermd worden voor inzage van onbevoegden en/of configurabel worden gemaakt zodat de instellingen dit zelf kunnen bepalen.	
Bewustwordingscampagne naar onderwijsinstellingen om de risico's van de vrije velden helder te maken.	Gereed 30 september 2025
Opvolgen van de onderzoeksresultaten	Gereed 31 maart 2026

Gemiste kansen en verlies van vertrouwelijkheid door handmatige invoer						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	Huidig risico
18.7	Handmatige invoer van verkeerde informatie	Gemiste lessen en gemiste kansen om ingeroosterd te worden	Redelijk	Enige	Midden	Huidig risico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	
	Training roosteraars	-	Laag	Enige	Laag	
	Automatiseren invoer waar mogelijk					

Mitigerende actie Xedule	Tijdslijn
Onderzoek welke velden relevant zijn voor notificatie van wijzigingen. Denk hierbij aan wijzigingen aan persoonsgegevens en roosterwijzigingen.	Gereed 31 oktober 2025
Implementatie van het onderzoeksresultaat	Gereed 31 maart 2026
Notificatie roosterwijzigingen	Gereed

Verlies van controle en vertrouwelijkheid door niet automatisch te configureren bewaartermijnen						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	Huidig risico
18.8	Geen automatische bewaartermijnen	Verlies van controle en vertrouwelijkheid	Hoog	Hoog	Hoog	Restrisico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	
	Vaststellen en beheren bewaartermijnen persoonsgegevens	Technische configuratie en beheer van bewaartermijnen per groep persoonsgegevens faciliteren	Laag	Hoog	Laag	
	Naleving bewaartermijnen vastleggen in processen	Inzichtelijk maken procedure verwijderen persoonsgegevens door middel van een verzoek aan Xedule				

Mitigerende actie Xedule	Tijdslijn
Onderzoek naar mogelijkheden om configureerbaar maken van de applicatie zodat de instellingen zelf de bewaartermijn kunnen instellen (al dan niet verplicht) waarbij het detailleren van verwijderen van gegevens die niet langer noodzakelijk zijn, onderdeel hiervan uitmaakt. Denk hierbij aan het categoriseren van persoonsgegevens e.d.	Gereed 31 december 2025
Implementatie van de technische maatregelen om de resultaten	Gereed 31 maart 2026
<i>Aanvullend: Op dit moment kan een onderwijsinstelling een verzoek doen waaraan direct gehoor gegeven wordt om de onderwijsinstelling te ondersteunen bij het verwijderen van de gevraagde gegevens.</i>	

Niet uit kunnen oefenen van AVG-rechten door incomplete inzageverzoeken						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	Huidig risico
18.9	Incomplete inzageverzoeken	AVG-rechten niet kunnen uitoefenen	Waarschijnlijk	Zwaar	Hoog	Restrisico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	
		Volledige inzage in verwerkingen verschaffen bij een inzageverzoek, bijvoorbeeld door beheerders de mogelijkheid te bieden zelf inzage te krijgen of door een duidelijke procedure te implementeren om inzageverzoeken te verwerken	Laag	Zwaar	Laag	

Mitigerende actie Xedule	Tijdslijn
Onderzoek welke mogelijkheden er zijn om betrokkenen zelf inzage te bieden waarbij gekeken dient te worden op welk vlak eigen inzage noodzakelijk is (er zijn niet veel leveranciers die deze mogelijkheid bieden).	Gereed 31 december 2025
Bekendheid geven aan het mogelijk maken van inzageverzoeken (procedure/informatie) zodat elke betrokkene zich kan vergewissen hoe rechten uitgeoefend kunnen worden met ondersteuning voor de functioneel beheerder. Denk hierbij aan het bekendmaken op de website en de in de online help	31 oktober 2025
Procedure inzageverzoek inrichten	Gereed
<i>Procedure om inzageverzoeken tijdig en correct af te handelen is inmiddels beschikbaar en kan getoetst worden door een inzageverzoek (op verzoek van SURF is gekozen voor ergens start schooljaar 25/26)</i>	

Verlies van controle en vertrouwelijkheid door het niet hebben van automatische import/export						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risico-score	Huidig risico
18.10	Handmatige import/export	Verlies van controle en vertrouwelijkheid	Redelijk	Zwaar	Hoog	Restrisico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risico-score	
	Waar mogelijk automatische koppeling met bronsystemen maken	Optie van automatisch import/export uitlichten en aanraden waar mogelijk	Laag	Zwaar	Laag	
	Duidelijke training en instructie voor degenen die gebruik moeten maken van handmatige import/export	Automatische import/export faciliteren waar mogelijk				

Mitigerende actie Xedule	Tijdslijn
Bewustwordingscampagne naar instellingen rondom het gebruik van import/export mogelijkheden met nadruk op automatische import/export mogelijkheden (koppelingen)	Gereed 30 september 2025
Informatiecampagne over het gebruik van handmatige import/export mogelijkheden waaronder het beschermen van informatie door het gebruik van templates (vast format om in te kunnen lezen) waardoor geen verkeerde info ingelezen kan worden.	Gereed 30 september 2025
Automatische import/export mogelijkheden daar waar mogelijk (koppelingen met applicaties)	Gereed
<i>Handmatige Importmogelijkheden zijn beschermd door middel van templates zodat een eenduidige werkwijze van importeren van informatie mogelijk is. Verkeerd bewerkte informatie kan niet ingelezen worden waarmee integriteit van de gegevens geborgd is.</i>	

Verlies van controle en vertrouwelijkheid door tabellen						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	Huidig risico
18.11	Configuratie van tabellen waardoor kopiëren en exporteren mogelijk is	Verlies van controle en vertrouwelijkheid	Redelijk	Zwaar	Hoog	Restrisico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	

	Duidelijke instructie voor gebruikers dat er geen gegevens geëxporteerd mogen worden, tenzij hier een goede (van tevoren bepaalde) reden voor is	Configuratiemogelijkheden bieden om de optie om gegevens uit tabellen te kopiëren en exporteren gericht uit te schakelen	Laag	Zwaar	Laag	
--	--	--	------	-------	------	--

Mitigerende actie Xedule	Tijdslijn
Onderzoek welke tabellen relevant zijn om te blokkeren of configurabel te maken om data te kopiëren.	31 december 2025
Resultaten implementeren	31 maart 2026
Bewustwordingscampagne die wijst op de risico's dat deze informatie gekopieerd kan worden.	30 september 2025

Verlies van vertrouwelijkheid door handmatige RBAC						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	Huidig risico
18.12	Alleen handmatige RBAC in applicaties	Verlies van vertrouwelijkheid	Redelijk	Zwaar	Hoog	Restrisico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	
	Richt processen in voor beheren van rollen en monitor de implementatie daarvan (RBAC)	Ondersteun een geautomatiseerde koppeling met externe identiteits- en toegangsbeheersystemen	Laag	Zwaar	Laag	
	Implementeer een centraal systeem voor beheren rechten					

Mitigerende actie Xedule	Tijdslijn
Informerende onderwijsinstellingen over het gebruik van Identity Access Management (IAM) om veiliger rechten uit te delen vanuit één enkel systeem	30 november 2025
Onderzoek beschikbaar stellen mogelijkheden tot centrale RBAC d.m.v. bijvoorbeeld een API koppeling aan te bieden.	30 november 2025
Inrichten oplossing zoals bijvoorbeeld de API (of andere uitkomst vanuit onderzoek)	31 maart 2026

Verlies van vertrouwelijkheid door onduidelijke configuratiewijzigingen						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	Huidig risico
18.13	Onduidelijke configuratiewijzigingen	Verlies van controle en vertrouwelijkheid	Redelijk	Zwaar	Hoog	Restrisico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	

	Maak deze instellingen alleen beschikbaar aan medewerkers die training hebben gehad over het gebruik ervan	Richt de interface op een manier die onbewuste autorisatiefouten tegengaat, bijvoorbeeld door visueel duidelijk te maken voor gebruikers welke autorisatiewijzigingen er zijn doorgevoerd	Laag	Zwaar	Laag	
--	--	---	------	-------	------	--

Mitigerende actie Xedule		Tijdslijn
Onderzoek of de huidige manier van autoriseren onbedoelde bijwerkingen hebben die niet zichtbaar zijn na de wijziging.		31 december 2025
Inregelen maatregelen vanuit het onderzoek		31 maart 2025

Verlies van vertrouwelijkheid door Xedule rest API						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	Huidig risico
18.14	Toegang zonder onderscheid door Xedule rest API	Verlies van controle en vertrouwelijkheid	Redelijk	Zwaar	Hoog	Restrisico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	
	Geef andere systemen alleen de minimaal benodigde toegang tot persoonsgegevens in de applicaties	Wijzig het autorisatiemodel van de API, zodat de toegang door een ander systeem tot een dataset beperkt kan worden tot de minimaal benodigde set	Laag	Zwaar	Laag	

Mitigerende actie Xedule	Tijdslijn
Ontwikkeling van een API-platform is inmiddels afgerond en beschikbaar en kan als mitigerende maatregel ingezet worden op verzoek van instellingen	Gereed start schooljaar om de instellingen te informeren rondom de risico's van de REST API's en de manier van werken.
Instellingen actief benaderen met de risico's op het gebruik van de REST API's e.d.	
Bewustwording omtrent het gebruik van API's waarbij actief aangestuurd wordt op het beëindigen van SOAP en de werkwijze rondom REST API's en aanvullende mogelijkheden	Gereed 31 oktober 2025

Verlies van vertrouwelijkheid en controle door ongeautoriseerde toegang door verouderde SOAP API						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	Huidig risico
18.15	Ongeautoriseerde toegang door verouderde SOAP API	Verlies van controle en vertrouwelijkheid	Redelijk	Zwaar	Hoog	Restrisico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	

	De SOAP API koppeling uitsfaseren	Ondersteuning van de SOAP API uitsfaseren	Laag	Zwaar	Laag	
--	-----------------------------------	---	------	-------	------	--

Mitigerende actie Xedule			Tijdslijn			
Uitsfaseren SOAP API (Actief EOL beleid richting de ene klant die het nog gebruikt).			Gereed Q3 2025 (begin schooljaar)			

Heridentificering van gepseudonimiseerde gegevens door gebrekkige anonimiseringsmethode						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	Huidig risico
18.16	Onjuiste anonimiseringsmethode	Heridentificering betrokkenen	Redelijk	Zwaar	Hoog	Restrisico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	
	AVG-waarborgen toepassen op door Xedule gepseudonimiseerde persoonsgegevens	In de dienstverlening duidelijk maken dat het om pseudonimisering gaat	Laag	Midden	Laag	Restrisico

Mitigerende actie Xedule			Tijdslijn			
Onderzoek naar een gegarandeerde mogelijkheid tot anonimisering.			Gereed Q3 2025			
Een statement voor verregaande pseudonimisering met de waarschijnlijkheid van anonimisering maar zonder garanties.			Gereed Q4 2025			

Heridentificering gepseudonimiseerde pNPS-gegevens						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	Huidig risico
Fout! Verwijzingsbron niet gevonden.	Onduidelijkheid over pseudonimiseringsmethoden	Heridentificering persoonsgegevens betrokkenen	Waarschijnlijk	Enige	Hoog	Restrisico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	
	Maak gebruik van de opt-out zolang er geen opt-in mechanisme is	Verander het mechanisme naar opt-in Implementeer aantoonbare maatregelen om heridentificatie te voorkomen	Laag	Enige	Laag	Restrisico

Mitigerende actie Xedule			Tijdslijn			
Onderzoek om opt-in bij pNPS aan te zetten.			Gereed Q4 2025			
Implementatie onderzoeksresultaten			Gereed 31 maart 2026			
Betere beschrijving pNPS verwerking inclusief controles op de werking van het mechanisme en het gebruik van AI			Gereed Q4 2025			

Verlies van vertrouwelijkheid door door ontbreken 'read access logging'						
Referentie	Aanleiding	Gevolg	Kans	Impact	Risicoscore	Huidig risico
18.18	Ontbreken read access logging	(Verder) verlies van vertrouwelijkheid	Waarschijnlijk	Zwaar	Hoog	Restrisico
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	
	Gebruik maken van de read access logs wanneer nodig	Read access logging implementeren	Laag	Zwaar	Laag	Restrisico

Mitigerende actie Xedule	Tijdstip
Diverse documenten en statements aanpassen met overzicht welke logging er plaatsvindt.	31 december 2025
Diverse documenten en statements aanpassen met overzicht welke persoonsgegevens verzameld worden met welk doel en grondslag	31 december 2025
Opzetten SIEM oplossing	Gereed 31 maart 2025

Conclusie

Deze DPIA heeft zeventien hoge risico's en één middenrisico gevonden bij het gebruik van Xedule en My Xedule. Voor al deze risico's zijn maatregelen voorgesteld die het risiconiveau naar laag brengen, zowel aan de kant van de instellingen als aan de kant van Xedule.

Xedule heeft concrete, realistische voorstellen gedaan om grotendeels in 2025 en voor een klein deel in 2026 invulling te geven aan deze maatregelen. Aangezien er zicht is op het mitigeren van de hoge risico's binnen een acceptabele termijn, kan het gebruik van Xedule en My Xedule daarom voorlopig worden voortgezet. In 2026 zal SURF een bijgewerkte versie van de DPIA met een nieuw advies publiceren.

20 Bijlage 1: Resultaten technische analyse

20.1 Onderschepte data

Voorbeeld telemetrie Microsoft Azure Application Insights

HTTP Request Header Analysis

POST /v2/track HTTP/2	# Endpoint for sending telemetry data to Azure
Host: dc.services.visualstudio.com	# Azure Application Insights collection endpoint
Content-Length: 7994	# Size of the payload in bytes
User-Agent: Mozilla/5.0...	# Browser information showing Chrome 131 on Windows
Sec-Ch-Ua-Platform: "macOS"	# Operating system platform identifier
Accept-Language: en-GB,en;q=0.9	# User's language preferences
Content-Type: application/json	# Data format of the request
Sdk-Context: appld	# Application context identifier

Telemetry Data Structure Analysis

"time": "2024-12-03T07:58:48.899Z",	# Timestamp of the telemetry event
"iKey": "c685eb91-5a1f-41b7-a7ad-8bd750662efd",	# Instrumentation key identifying your app instance

"name": "Microsoft.ApplicationInsights.[...].RemoteDependency",	# Type of telemetry being sent
--	--------------------------------

"tags": {	# Metadata tags for the request
"ai.user.id": "Z7wY16OJ9dsJ6pyqUEBirY",	# Unique identifier for the user
"ai.session.id": "mwzpwFmRg2JODGBH7PM5Et",	# Unique identifier for the session

"ai.device.id": "browser",	# Device type identifier
"ai.device.type": "Browser",	# Device category
"ai.operation.name": "/roster/overview/schedule/mine",	# Route or operation being tracked
"ai.operation.id": "e3ba68db343f4b878327fea5206fa19d",	# Unique operation identifier
"ai.internal.sdkVersion": "javascript:3.3.4"	# Version of Application Insights SDK

Actual telemetry data

"baseType": "RemoteDependencyData",	# Type of data being collected
-------------------------------------	--------------------------------

"id": " e3ba68db343f4b878327fea5206fa19d.9065d99f4da848f2.",	# Unique request identifier
"ver": 2,	# Version of the data format
"name": "GET /api/Appointment/Date/2024-11-13/2024-12-02/Attendee?id=14573",	# API endpoint called
"resultCode": "200",	# HTTP response code
"duration": "00:00:00.169",	# How long the request took
"success": true,	# Whether the request succeeded
"data": "GET /api/Appointment/Date/2024-11-13/2024-12-02/Attendee?id=14573",	# Request details
"target": "surf-test.myx.nl cid-v1:d5f00470-89fd-4fc9-b5ea-ee4ff7c63543",	# Target service
"type": "Ajax",	# Type of dependency call

"HttpMethod": "GET"	# HTTP method used
---------------------	--------------------

"measurements": {}	# Custom measurements (empty in this case)
--------------------	---

20.2 Test scenario's

In deze sectie zijn alle test cases beschreven die uitgevoerd dienen te worden met behulp van een man-in-the-middle proxy, bijvoorbeeld Burp Suite of mitmproxy. Bij het uitvoeren van de testen, zorg ervoor dat er ongeveer ~10 seconden tussen de stappen zitten.

TC-01 – Authentiseren in My Xedule

Test Case ID	TC-01
Use Case	Authentiseren
Actor(s)	Student, Docent, Leidinggevende

Preconditions

- De testomgeving is ingericht volgens hoofdstuk **Fout! Verwijzingsbron niet gevonden..**
- De testomgeving is bereikbaar.
- De actors zijn al eerder ingelogd geweest.
- De internetbrowser heeft geen opgeslagen gegevens (cookies, cache, etc.)

Steps

1. Start de proxy.
2. Navigeer naar de loginpagina van My Xedule
3. Log in met een actor.
4. Wacht tot de startpagina van My Xedule
5. Stop de proxy.

Opmerkingen:

- Herhaal bovenstaande stappen voor de actoren: Student A, Docent A en Leidinggevende.

TC-02 – Authentiseren in Xedule

Test Case ID	TC-02
--------------	-------

Use Case	Authentiseren
Actor(s)	Roostermaker

Preconditions

- De testomgeving is ingericht volgens hoofdstuk **Fout! Verwijzingsbron niet gevonden..**
- De testomgeving is bereikbaar.
- De roostermaker is al eerder ingelogd geweest.
- De roostermaker heeft een sessie genaamd “Nieuwe sessie”.
- De internetbrowser heeft geen opgeslagen gegevens (cookies, cache, etc.)

Steps

6. Start de proxy.
7. Navigeer naar de loginpagina van Xedule
8. Log in als Roostermaker.
9. Selecteer de bestaande sessie “Nieuwe sessie”.
10. Wacht tot de startpagina van Xedule geladen is.
11. Stop de proxy.

TC-03 – Docent ziekmelden

Test Case ID	TC-03
Use Case	Ziekmelden
Actor(s)	Docent, Roostermaker

Preconditions

- De testomgeving is ingericht volgens hoofdstuk **Fout! Verwijzingsbron niet gevonden..**
- De testomgeving is bereikbaar.
- De Roostermaker is ingelogd en staat op de startpagina van Xedule.
- Docent (A) heeft zichzelf ziekgemeld bij de leidinggevende of direct aan de Roostermaker buiten Xedule om (fictieve werkomschrijving).

Steps

1. Start de proxy.
2. Navigeer naar “Dagroosterbeheer” > “Conflicten invoeren”.
3. Voer een nieuw conflict in met de code “bruir_ziek” vanaf 19-08-2024 t/m 30-11-2024.
4. Voeg Docent (A) aan het conflict toe.
5. Ga naar “Dagroosterbeheer” > “Conflicten oplossen”.
6. Klik op “bruirn_ziek” en vervolgens op “Les(sen) uitroosteren”.
7. Stop de proxy.

TC-04 – Docent geeft beschikbaarheid door

Test Case ID	TC-04
Use Case	Doorgeven beschikbaarheid
Actor(s)	Docent, Leidinggevende

Preconditions

- De testomgeving is ingericht volgens hoofdstuk **Fout! Verwijzingsbron niet gevonden..**
- De testomgeving is bereikbaar.
- Docent (A) en Leidinggevende zijn ingelogd.
- Docent (A) staat op de startpagina van My Xedule.
- De Leidinggevende staat op de startpagina van My Xedule.

Steps

1. Start de proxy.
2. Docent (A) navigeert naar de pagina voor doorgeven van beschikbaarheid.
3. Docent (A) selecteert Maandag t/m Donderdag, behalve Woensdag tussen 08-00-12.15 en klikt op Verder.
4. Docent (A) vult bij Woensdag 08.00 – 08.30 als opmerking in “In de ochtend niet beschikbaar vanwege fysiotherapie.” en klikt op Verder.
5. Docent (A) klikt op Indienen.
6. Leidinggevende navigeert naar de pagina voor controleren aanvragen medewerkers.
7. Leidinggevende opent melding van Docent (A).
8. Leidinggevende keurt goed.
9. Stop de proxy.

TC-06 – Bekijken eigen rooster docent

Test Case ID	TC-06
Use Case	Bekijken rooster
Actor(s)	Docent

Preconditions

- De testomgeving is ingericht volgens hoofdstuk **Fout! Verwijzingsbron niet gevonden..**
- De testomgeving is bereikbaar.
- Docent (A) is ingelogd en staat op de startpagina van My Xedule.

Steps

1. Start de proxy.
2. Navigeer naar het rooster.
3. Klik op een willekeurig roosteritem om meer details in te zien.
4. Sluit het roosteritem af.
5. Herhaal stap 3 en 4 voor nog twee roosteritems.
6. Stop de proxy.

TC-07 – Bekijken rooster andere docent

Test Case ID	TC-07
Use Case	Bekijken rooster
Actor(s)	Docent

Preconditions

- De testomgeving is ingericht volgens hoofdstuk **Fout! Verwijzingsbron niet gevonden..**
- De testomgeving is bereikbaar.
- Docent (B) is ingelogd en staat op de startpagina van My Xedule.

Steps

1. Start de proxy.
2. Navigeer naar het rooster.
3. Open het rooster van Docent (A).
4. Klik op een willekeurig roosteritem om meer details in te zien.

5. Stop de proxy.

TC-09 – Exporteren rooster naar ICS

Test Case ID	TC-09
Use Case	Bekijken rooster
Actor(s)	Student

Preconditions

- De testomgeving is ingericht volgens hoofdstuk **Fout! Verwijzingsbron niet gevonden..**
- De testomgeving is bereikbaar.
- Student (A) is ingelogd en staat op de startpagina van Xedule (rooster) en staat in een week waar lessen gepland zijn.

Steps

1. Start de proxy.
2. Navigeer naar het rooster.
3. Exporteer het rooster naar ICS.
4. Download de ICS.
5. Stop de proxy.

TC-10 – Bekijken eigen rooster student

Test Case ID	TC-10
Use Case	Bekijken rooster
Actor(s)	Student

Preconditions

- De testomgeving is ingericht volgens hoofdstuk **Fout! Verwijzingsbron niet gevonden..**
- De testomgeving is bereikbaar.
- Student (A) is ingelogd en staat op de startpagina van My Xedule (rooster)

Steps

1. Start de proxy.
2. Navigeer naar de week van 25 nov – 29 nov.

3. Klik op een roosteritem om meer details in te zien.
4. Sluit het roosteritem af.
5. Herhaal stap 3 en 4 voor nog twee roosteritems.
6. Stop de proxy.

TC-11 – Aanpassen persoonlijke instellingen

Test Case ID	TC-10
Use Case	Bekijken rooster
Actor(s)	Student

Preconditions

- De testomgeving is ingericht volgens hoofdstuk **Fout! Verwijzingsbron niet gevonden..**
- De testomgeving is bereikbaar.
- Student (A) is ingelogd en staat op de startpagina van My Xedule (rooster).
- De taal van Student (A) staat op Nederlands.
- Het thema van Student (A) staat op Donker.

Steps

1. Start de proxy.
2. Ga naar Instellingen via de drie puntjes naast de naam van Student (A).
3. Pas de taal aan naar English.
4. Pas het thema aan naar Light.
5. Stop de proxy

20.3 Voorbeeld inzageverzoek

Zie volgende pagina.

Identiteitsverificatie

Selecteer de van toepassing zijnde betrokkene:

- ☐ Regulier account
- ☐ Testaccount of onderzoekaccount

Details Verificatie

Voor Test- en Onderzoekaccounts

Project referentie: **CA-Xedule**

Testscenario ID: **TC-01, TC-03, TC-04, TC-06, TC-07**

Account credentials

Gebruikersnaam/ID: **XXXXX**

Gebruikersnaam/ID: **XEDULE\surf_XXXXX**

Rol in onderzoek: **Docent**

<https://surf-test.xedule.nl>

<http://surf-test.myx.nl/xedule>

Bevestiging onderzoeksscope

Dit account is onderdeel van het formele onderzoek, **Compliance Assessment Xedule door SURF** dat van **3 december tot en met 17 december 2024** heeft gelopen ter ondersteuning van de Gegevens Effecten Beoordeling.

Goedkeuring is gegeven door testcoördinator ##### & #####.

Details Verzoek

Tijdsperiode

Gelieve informatie te verstrekken voor de volgende periode van **3 december 2024** tot en met **17 december 2024**.

Reikwijdte Verzoek

Ik verzoek om een kopie van:

- Alle persoonsgegevens die u over eerder gespecificeerd account/persoon (heeft) verwerkt
- Specifieke gegevenscategorieën (hieronder gespecificeerd)

Gevraagde Specifieke Gegevenscategorieën

Gelieve de volgende gegevenscategorieën op te nemen, maar niet te beperken tot:

Accountinformatie

- Gebruikersprofielgegevens
- Accountinstellingen
- Registratie-informatie
- Primary Key van de gebruiker

Activiteitengegevens

- Inloggeschiedenis
- Systeeminteracties
- Transactiegegevens
- Gebruikslogboeken

Technische Gegevens

- Apparaatinformatie
- IP-adressen
- Sessiegegevens
- Technische identificatoren

Aanvullende Informatie

Om mijn informatie te lokaliseren zijn de volgende gegevens relevant:

Accounts:

Username: XXXXX
 Username: XEDULE\surf_XXXXX
 Emailadres: surf_XXXXX@xedule.nl

ID's

ai_user: #####
 ai_session: #####
 ASP.NET_SessionId: #####

IP-adressen

3-12: 145.90.###.##
 16-12: 85.147.##.##

Tabel 20-1, voorbeel inzageverzoek.



21 Bijlage 2: persoonsgegevens

Persoonsgegevens	Categorieën betrokkenen	Categorie persoonsgegevens	Gevoeligheid persoonsgegevens	Bron	Onderwijsplanning Rooster	Authenticatie/Identificatie	Backup en gegevensherstel	Personalisering	Klantondersteuning	Verwerking van planafwijking	Fraudepreventie
Voornaam	Docent, Student, Medewerker	Contactgegevens	Gewoon	HR-systeem / import		X					
Achternaam	Docent, Student, Medewerker	Contactgegevens	Gewoon	HR-systeem / import		X					
Gebruikersnaam/personeelsnummer	Docent, Student, Medewerker	Contactgegevens	Gewoon	HR-systeem / import		X					
E-mailadres	Docent, Student, Medewerker	Contactgegevens	Gewoon	HR-systeem / import		X					
Geboortedatum	Docent, Student, Medewerker	Demografische gegevens	Gewoon	HR-systeem / import							
Referentie ID	Docent, Student, Medewerker	Contactgegevens	Gewoon	HR-systeem / systeem / import		X					
Roostervoorwaarden en beschikbaarheid	Docent, Student	Organisatiegegevens	Gewoon	HR-systeem / systeem / import	X	X					
Opleiding, klas/lesgroepnummer	Docent, Student	Organisatiegegevens	Gevoelig	HR-systeem / systeem / import	X	X					
Onderwijsproducten en bijbehorende toetsen	Docent, Student	Organisatiegegevens	Gewoon	HR-systeem / systeem / import	X	X					
Locatiegegevens (faciliteit en klaslokaal)	Docent, Student	Locatiegegevens	Gevoelig	HR-systeem / facilitair systeem / import	X						
Indiensttreding	Docent, Student, Medewerker	Organisatiegegevens	Gevoelig	HR-systeem / systeem / import	X						
Bron organisatorisch eenheid	Docent, Student, Medewerker	Organisatiegegevens	Gewoon	HR-systeem / systeem / import	X						
Verlofuren (bijzonder verlof, adoptieverlof, buiten)	Docent	Gezondheidsgegevens	Gevoelig	HR-systeem / systeem / import	X						
Medewerkerstype	Docent, Medewerker	Organisatiegegevens	Gewoon	HR-systeem / systeem / import	X						
Hoofdtteam of onderwisteam	Docent, Medewerker	Organisatiegegevens	Gewoon	HR-systeem / systeem / import	X						
Contracttype (Type arbeidsovereenkomst (Bepaald))	Docent, Medewerker	Organisatiegegevens	Gevoelig	HR-systeem / systeem / import	X						
Voorkeursfaciliteiten	Docent	Organisatiegegevens	Gewoon	HR-systeem / systeem / import		X					
Expertises	Docent	Organisatiegegevens	Gewoon	HR-systeem / systeem / import	X	X					
Loginformatie	Docent, Student, Medewerker	Technische gegevens	Gewoon	Systeem				X	X	X	
Koppeling MyXedule	Docent, Student, Medewerker	Technische gegevens	Gewoon	Systeem		X					
Aanvullende rol als coach	Docent	Organisatiegegevens	Gewoon	HR-systeem / systeem / import		X					
Taken	Docent	Organisatiegegevens	Gewoon	HR-systeem / systeem / import	X	X					
Hulpmiddelen	Student	Gezondheidsgegevens	Bijzonder	Handmatig		X					
Logbestanden	Docent, Student, Medewerker	Technische gegevens	Gewoon	Systeem				X	X	X	
Systeemfouten	Docent, Student, Medewerker	Technische gegevens	Gewoon	Systeem				X	X	X	
Gebruikte applicatie	Docent, Student, Medewerker	Technische gegevens	Gewoon	Systeem				X	X	X	
Tijdstip van gebruik	Docent, Student, Medewerker	Technische gegevens	Gewoon	Systeem				X	X	X	
Webbrowser en webbrowser versie	Docent, Student, Medewerker	Technische gegevens	Gewoon	Systeem				X	X	X	
Besturingssysteem	Docent, Student, Medewerker	Technische gegevens	Gewoon	Systeem				X	X	X	
Apparaat (telefoon, tablet, computer)	Docent, Student, Medewerker	Technische gegevens	Gewoon	Systeem				X	X	X	
Authenticatieresultaat	Docent, Student, Medewerker	Technische gegevens	Gewoon	Systeem		X					X
IP-adres	Docent, Student, Medewerker	Technische gegevens	Gewoon	Device betrokkene				X	X	X	
Cookies	Docent, Student, Medewerker	Technische gegevens	Gewoon	Systeem		X					
Demografische informatie tot op het niveau van	Docent, Student, Medewerker	Locatiegegevens	Gewoon	Device betrokkene				X	X	X	
Werktijdfactor	Docent	Organisatiegegevens	Gewoon	HR-systeem / systeem / import	X						
Instellingsvoorkeuren	Docent, Student, Medewerker	Technische gegevens	Gewoon	Handmatig				X			

22 Bijlage 3: MORA vergeleken met HORA

In onderstaande tabel is een vergelijking gemaakt tussen de processen beschreven in het Hoger Onderwijs Referentie Architectuur⁴⁴ (HORA) en het Middelbaar Beroeps Onderwijs Referentie Architectuur⁴⁵ (MORA). Deze processen zijn daaronder uitgeschreven conform deze referentie architectuur.

HORA	MORA
Onderwijsplanning	
Onderwijsadministratie	Maken jaarplanning
Onderwijseenheidsinschrijving	Aanmelden geroosterde activiteit
Toetsinschrijving	
Vraagprognosisering	Maken jaarplanning, Analyseren werkverdeling, Analyseren middelen, Maken meerjaren planning
Lesgroepvorming	Maken jaarplanning
Inzet- en middelenplanning	Matchen beschikbare mensen en middelen op de onderwijsvraag
Onderwijsactiviteitenplanning	Maken jaarplanning
Roosteren	
Lesroosterconstructie	Clusteren leeractiviteiten, Maken rooster, Jaarkalender vaststellen, Afhandelen niet planbare leerroutes
Roosterwijziging	Beheren rooster wijzigingen
Roosterpublicatie	Publiceren rooster
Toetsroosterconstructie	Maken examenplanning

Tabel 22-1, vergelijking HORA en MORA

⁴⁴ <https://hora.surf.nl/index.php/Hoofdpagina>

⁴⁵ <https://mora.mbo.digitaal.nl/index.php/Hoofdpagina>

Voor deze verwerking relevante processen beschreven in HORA⁴⁶

Onderwijsplanning

Onderwijsadministratie:

De administratieve ondersteuning van de ontwikkeling van het onderwijs, inclusief het publiceren van een OER en de studiegids.

Bijvoorbeeld: Beheer van onderwijsdocumentatie, faciliteren transparantie voor studenten en medewerkers.

Onderwijseenheidsinschrijving:

Het (impliciet of expliciet) inschrijven van een deelnemer voor een onderwijseenheid.

Bijvoorbeeld: Zowel handmatige als geautomatiseerde inschrijvingsprocessen, waarborgen van accurate deelnemersregistratie.

Toetsinschrijving:

Het (impliciet of expliciet) inschrijven van een deelnemer voor toetsactiviteiten.

Bijvoorbeeld: Beheer van toetsdeelname, capaciteitsplanning, administratieve ondersteuning.

Vraagprognosisering:

Het maken van een prognose van de hoeveelheid deelnemers en de onderwijsproducten die zij willen afnemen (studentenplanning).

Bijvoorbeeld: Datagedreven besluitvorming, resource management.

Lesgroepvorming:

Het samenstellen van groepen van deelnemers ten behoeve van het gezamenlijk volgen van onderwijseenheden.

Bijvoorbeeld: Balanceren van groepsgrootte, leerdoelen, beschikbare faciliteiten.

Inzet- en middelenplanning:

Het reserveren van capaciteit van mensen en middelen zodat zij beschikbaar zijn om te voldoen aan de geprognosticeerde vraag

Bijvoorbeeld: Personeelsinzet, lokaaltoedeling, apparatuur reservering.

Onderwijsactiviteitenplanning:

Het inplannen van de specifieke activiteiten die in het kader van een onderwijseenheid noodzakelijk zijn, inclusief het bepalen van de vorm waarin de activiteit zal plaatsvinden (zoals een stage).

Bijvoorbeeld: Flexibiliteit in onderwijsvormen, stage-coördinatie.

⁴⁶ <https://hora.surf.nl/index.php/Hoofdpagina>

Roosteren

Lesroosterconstructie:

Het koppelen van mensen, middelen en leeractiviteiten op bepaalde momenten in tijd.

Bijvoorbeeld: Minimaliseren conflicten, maximaliseren beschikbaarheid.

Roosterwijziging:

Het aanbrengen van correcties in het rooster zodat deze beter past op de daadwerkelijke beschikbaarheid van mensen en middelen.

Bijvoorbeeld: Real-time aanpassingen, communicatie van wijzigingen.

Roosterpublicatie:

Het beschikbaar stellen van het rooster aan alle relevante doelgroepen.

Bijvoorbeeld: Multikanaal communicatie, gebruiksvriendelijke interfaces.

Toetsroosterconstructie:

Het koppelen van mensen, middelen en toetsactiviteiten op bepaalde momenten in tijd.

Bijvoorbeeld: Concrete aspecten: Capaciteitsbeheer, logistieke ondersteuning.

Voor deze verwerking relevante processen beschreven in MORA⁴⁷

Plannen en Roosteren

Aanmelden geroosterde activiteit

In het gepubliceerde rooster kunnen leertaken zijn geroosterd waarvoor studenten zich kunnen aanmelden. Dit kan onderdeel zijn van hun persoonlijke leerroute.

De student moet zich actief aanmelden voor zo'n geroosterde module, bijvoorbeeld omdat er een maximumaantal studenten kan worden toegelaten, of omdat studenten aan bepaalde voorwaarden moeten voldoen.

Afhandelen niet planbare leerroutes

Het kan voorkomen dat leerroutes (of delen ervan) 'niet planbaar' zijn doordat te weinig studenten hiervoor kiezen, er te weinig middelen beschikbaar zijn of omdat de gestelde randvoorwaarden door de student fricties opleveren met de randvoorwaarden van een opleidingsonderdeel of leertaak. Deze leerroutes zijn niet, of niet geheel in het rooster opgenomen.

Er wordt een oplossing gezocht voor de niet geplande leerroutes, al dan niet met aanpassing van de leervraag of de leerroute door bijvoorbeeld het kiezen van alternatieve opleidingsonderdelen of leertaken die in een komende periode wel worden aangeboden.

Beheren rooster wijzigingen

⁴⁷ <https://mora.mbodigitaal.nl/index.php/Hoofdpagina>

Er zijn situaties denkbaar dat het rooster veranderd moet worden ook al is dit vastgesteld voor een bepaalde periode. Om dit probleem op te lossen kan het rooster of de inzet van middelen worden aangepast. Wijzigingen worden tijdig doorgegeven en verwerkt zodat studenten en docenten tijdig geïnformeerd worden.

Dit kan het gevolg zijn van een uitvoeringsprobleem, zoals:

- Ziekte van een docent
- Een docent is plotseling verhinderd of niet beschikbaar
- Een stageplaats is toch niet beschikbaar
- Noodzakelijke apparatuur (zoals PCs) zijn niet tijdig geleverd
- Wijzigingen in student-, klas- of groepssamenstellingen
- Wijzigingen in faciliteiten

Dit kan ook het gevolg zijn van een calamiteit, een onvoorziene omstandigheid. Dit kan qua omvang en impact zeer divers zijn, denk aan:

- Een docent is plotseling langdurig afwezig
- Alle PC's zijn uit een lokaal gestolen
- Brand of lekkage

Clusteren leeractiviteiten

Het clusteren van leeractiviteiten is het samennemen van verschillende leeractiviteiten die in een periode gelijktijdig/naast elkaar uitgevoerd zullen worden. Dit is nodig om het onderwijs te kunnen organiseren en zowel medewerkers als voorzieningen efficiënt te kunnen inzetten. Deze processtap is een belangrijke schakel in de overgang van meerjarenplanning naar jaarplanning en concrete roosters.

Per opleiding vormen alle leeractiviteiten, gecombineerd tot opleidingsonderdelen, samen het onderwijsaanbod van die opleiding, over meerdere perioden en jaren heen. Er hoort een meerjarenplanning bij.

Leerroutes van studenten zijn opgebouwd uit opleidingsonderdelen. Deze opleidingsonderdelen bestaan uit leeractiviteiten die moeten worden gepland, soms parallel en soms opvolgend, ook over een langere periode.

De meerjarenplanning en de gekozen leerroutes van de studenten samen vormen nog geen geordend geheel dat in de vorm van roosters en planningen kan worden gegoten. De leeractiviteiten worden geclusterd in periodes waardoor er een geordend geheel ontstaat. De clustering van leeractiviteiten heeft invloed op de jaarplanning en de analyse van de werkverdeling.

Jaarkalender vaststellen

De instelling stelt jaarlijks een jaarkalender vast. In deze jaarkalender zijn de volgende zaken opgenomen:

- Start en einde schooljaar
- Vakanties
- Feestdagen
- Periodisering
- Examenweken

Het Ministerie van OCW levert een advies inzake de schoolvakanties. De jaarkalender biedt de basis voor het inplannen van het onderwijs in de jaarplanning.

Maken examenplanning

Het uitwerken van een planning voor de uitvoering van examens op basis van het examenplan en de jaarplanning

Maken jaarplanning

De jaarplanning is het resultaat van het matchen van het onderwijsaanbod, studenten, BPV, de medewerkers en de faciliteiten, grofmazig uiteengezet over het schooljaar (globaal jaarrooster) en indien van toepassing periodes. In voorkomende gevallen kan de instelling bijsturen op de genoemde onderdelen. Het maken van de jaarplanning kent een wisselwerking met het analyseren van de werkverdeling. Op basis van de jaarplanning wordt het plan van inzet voor de medewerkers samengesteld.

De jaarplanning wordt op basis van de volgende informatie ontwikkeld:

- Het beoogde onderwijsaanbod
- De schatting van het onderwijs en studenten
- De jaarkalender
- De analyse van de werkverdeling
- De analyse van de faciliteiten
- De clustering van leertaken

Het matchen van het onderwijsaanbod, studenten, BPV, de medewerkers en de middelen, grofmazig uiteengezet over het schooljaar (globaal jaarrooster) en indien van toepassing periodes. In voorkomende gevallen kan de instelling bijsturen op de genoemde onderdelen. Het maken van de jaarplanning kent een wisselwerking met het analyseren en opstellen van de werkverdeling. Op basis van de jaarplanning wordt het plan van inzet voor de medewerkers samengesteld.

In de jaarplanning wordt rekening gehouden met:

- Afspraken die voortvloeien uit de onderwijswetgeving (urennorm)
- Afspraken die voortvloeien uit de CAO MBO
- Afspraken die voortvloeien uit de OER
- De inhoud van de curricula

Bij wijzigingen in onderwijsaanbod, werkverdeling en faciliteitenbeschikbaarheid gedurende het schooljaar wordt de jaarplanning onderhouden.

De jaarplanning voedt het roosteren.

Maken rooster

Het roosteren van onderwijsactiviteiten op basis van de jaarplanning en het toetsen van het rooster aan de jaarplanning.

Dit omvat de matching tussen specifieke:

- Geclusterde leertaken
- (Arrangementen) van student(en)
- Klas(sen) of groep(en)
- Middelen
- Mensen (docent(en) en/of instructeurs)
- Datum en tijd

Het roosteren kan per schooljaar of per periode uitgevoerd worden.

Het rooster houdt rekening met:

- De onderwijswetgeving (urennorm) - de CAO MBO
- De OER

Matchen beschikbare mensen en middelen op de onderwijsvraag

Het matchen van de beschikbare medewerkers en middelen op de totale onderwijsvraag van de komende periode. Dit leidt tot het daadwerkelijk toewijzen van deze medewerkers en middelen aan te plannen leertaken.

Publiceren rooster

Het publiceren van het rooster voor studenten en docenten. Dit gebeurt periodiek en na wijzigingen.

Prognosticeren mensen- en middelen behoefte

Analyseren middelen

Op basis van het beoogde onderwijsaanbod wordt onderzocht of er voldoende faciliteiten aanwezig zijn. Hiertoe worden de huidige beschikbare faciliteiten geanalyseerd.

Hierbij wordt gelet op:

- Lokalen en ruimtes
- Beschikbare ICT-middelen
- Beschikbare beroepsgerichte middelen
- Onderwijsondersteunende materialen

Deze analyse wordt gebruikt in de jaarplanning.

Analyseren werkverdeling

Op basis van de inschatting van het aantal toekomstige studenten en onderwijs wordt een analyse gemaakt voor de werkverdeling. Deze analyse weergeeft de inzet van de medewerkers ten opzichte van de verwachte onderwijsvraag.

Dit kan leiden tot:

- Wijzigingen in het personeelsbestand
- Wijzigingen in het onderwijsaanbod
- Wijzigingen in de clustering van leertaken
- Wijzigingen in de jaarplanning

Deze analyse voedt en kent een wisselwerking met de jaarplanning.

Maken meerjaren planning

Een meerjarenplanning wordt opgesteld om inzicht te krijgen in de huidige en toekomstige faciliteiten en expertisebehoeften binnen een opleiding. Er wordt een match gemaakt tussen het onderwijsaanbod, de medewerkers en de faciliteiten. Dit wordt grofmazig uiteengezet over meerdere jaren. Deze planning is de basis voor het maken van leertaken die passen in de leerroutes van studenten.

De meerjarenplanning wordt gebaseerd op een schatting van het onderwijs en studenten, de curricula- of onderwijsplannen, faciliteitsgegevens en de medewerkersgegevens. De meerjarenplanning richt zich op het capaciteitsvraagstuk over het gehele curriculum van de studenten. Op deze manier biedt de meerjarenplanning handvatten voor het tijdig bijsturen van de instelling inzake het onderwijsaanbod, het faciliteitsaanbod en het personeelsbestand.