DPIA Xedule en My Xedule - Update

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

12 november 2026

Auteur(s): Sophia Gelpke & Jan Landsaat
Versie: 2.0
Datum: 12 november 2026

Deze publicatie is gelicenseerd onder een Creative Commons Naamsvermelding 4.0 Internationaal.

Inhoudsopgave

Versiegeschiedenis 7

1 Samenvatting 8

2 Inleiding 15

2.1 Noodzaak DPIA 15
2.2 Centrale DPIA door SURF 16
2.3 Model 17
2.4 Methodologie 18
2.5 Scope van deze DPIA 18
2.6 Out of scope 18

A. Beschrijving algemene kenmerken gegevensverwerkingen 20

3 Introductie Xedule 20

3.1 Xedule en Visma 20
3.2 Toelichting Xedule en My Xedule 21
3.2.1 Xedule *21*
3.2.2 My Xedule *22*
3.2.3 Proces *22*

4 Verwerkingsdoeleinden 24

4.1 Hoofddoelen instellingen (conform HORA) 24
4.1.1 Hoofddoel instellingen: Onderwijsplanning *24*
4.1.2 Hoofddoel instellingen: Roostering *25*
4.2 Verwerkingsdoeleinden instellingen verwerkersovereenkomst 26
4.3 Verwerkingsdoeleinden Xedule verwerkersovereenkomst 26

5 Persoonsgegevens 28

6 Gegevensverwerkingen 30

6.1 Roosteren & plannen van onderwijs 30
6.1.1 Geautomatiseerde verzameling *30*
6.1.2 Handmatige verzameling *32*
6.1.3 Opslag *39*
6.1.4 Datamanagement *39*
6.1.5 Publiceren *41*
6.1.6 Verwijdering van gegevens *42*
6.2 Beheer 43
6.2.1 Identiteits- en toegangsbeheer *44*
6.2.2 Configuratie *45*
6.3 Logging 45

6.3.1 Microsoft Azure Application Insights 47
6.4 Inzageverzoeken 48
6.4.1 Inzageverzoeken najaar 2024 48
6.4.2 Inzageverzoeken zomer 2026 49

7 Technieken en methoden van de gegevensverwerkingen 50

7.1 Software-as-a-Service 50
7.2 Geautomatiseerde besluitvorming 50
7.3 Backup 50
7.4 Pseudonimiseren 51
7.5 Anonimiseren / pseudonimiseren 52
7.6 Encryptie 52
7.6.1 Encryptie data in transit 52
7.6.2 Encryptie data at rest 52
7.7 API's 53
7.7.1 Gestandaardiseerde integratiemogelijkheden 53
7.7.2 Delen 54
7.8 Cookies 57
7.8.1 Xedule 57
7.8.2 My Xedule 57

8 Betrokken partijen 59

8.1 Onderwijsinstelling: Verwerkingsverantwoordelijke 59
8.2 Xedule: Verwerker 60
8.3 Xedule: Gemachtigd verwerkingsverantwoordelijke 60
8.4 Subverwerkers van Xedule 61
8.4.1 Interconnect 63
8.4.2 Zendesk Inc. via Contact Center Live 64
8.4.3 Synaxion B.V. 65
8.4.4 Microsoft Norge AS 65
8.4.5 ESCROW4ALL 65
8.5 Betrokkenen 66
8.6 Ontvangers 66
8.7 Verstrekkers 66
8.8 Derden 66

9 Belangen bij de gegevensverwerkingen 67

9.1 Onderwijsinstelling 67
9.2 Studenten 67
9.3 Medewerkers (Docenten) 68
9.4 Xedule 68

10 Verwerkingslocaties 69

10.1 Doorgiftes 69
10.1.1 Microsoft 69
10.1.2 Zendesk 71

10.2 Doorgiftemechanismes 71

11 Juridisch en beleidsmatig kader 72

11.1 Juridische en beleidsmatige kaders 72
11.2 Corporate Xedule beleid 73

12 Bewaartermijnen 74

12.1 Bewaartermijnen als verwerker 74
12.1.1 Xedule 74
12.1.2 Onderwijsinstelling 74
12.2 Bewaartermijnen als verwerkingsverantwoordelijke 75

B. Beoordeling rechtmatigheid gegevensverwerkingen 76

13 Rechtsgrond 76

13.1 Grondslagen instellingen 76
13.2 Grondslagen Xedule 77

14 Bijzondere persoonsgegevens 80

14.1 Medewerkers 80
14.2 Studenten 80

15 Doelbinding 82

15.1 Interne doelbinding 82
15.2 Doelbinding Xedule 82

16 Noodzaak en evenredigheid 83

16.1 Subsidiariteit 83
16.2 Proportionaliteit 83

17 Rechten van de betrokkenen 87

C. Beschrijving en beoordeling risico's voor betrokkenen 89

18 Risico's voor betrokkenen 89

18.1 Verlies van controle door Xedule als verwerkingsverantwoordelijke 90
18.2 Verlies van controle door gebrek aan transparantie logging, pNPS en marketing 91
18.3 Verlies van vertrouwelijkheid en sociaal nadeel door te brede definiëring afwezigheids- en hulpmiddelencategorieën 92
18.4 Niet mogelijk om AVG-rechten uit te oefenen en verlies van controle door gebrek aan transparantie subverwerkers 93

18.5 Verlies van vertrouwelijkheid door doorgeven beschikbaarheidsredenen aan roosteraars 94
18.6 Verlies van controle en vertrouwelijkheid door overige vrije velden 95
18.7 Gemiste kansen en verlies van vertrouwelijkheid door handmatige invoer 96
18.8 Verlies van controle en vertrouwelijkheid door niet automatisch te configureren bewaartermijnen 96
18.9 Niet uit kunnen oefenen van AVG-rechten door incomplete inzageverzoeken 97
18.10 Verlies van controle en vertrouwelijkheid door het niet hebben van automatische import/export 98
18.11 Verlies van controle en vertrouwelijkheid door tabellen 99
18.12 Verlies van vertrouwelijkheid door handmatige RBAC 99
18.13 Verlies van vertrouwelijkheid door onduidelijke configuratiewijzigingen 100
18.14 Verlies van vertrouwelijkheid door Xedule rest API 100
18.15 Verlies van vertrouwelijkheid en controle door ongeautoriseerde toegang door verouderde SOAP API 101
18.16 Heridentificering van gepseudonimiseerde gegevens door gebrekkige anonimiseringsmethode 101
18.17 Heridentificering gepseudonimiseerde pNPS-gegevens 102
18.18 Verlies van vertrouwelijkheid door door ontbreken 'read access logging' 103
18.19 NIEUW Verlies van controle door verplichte openbaarmaking of onbevoegde toegang in derde landen 104

D. Beschrijving voorgenomen maatregelen 105

19 Maatregelen 105

Conclusie 118

20 Bijlage 1: Resultaten technische analyse 119

20.1 Onderschepte data 119
20.2 Testscenario's 121
20.3 Testscenario's zomer 2026 126
20.4 Voorbeeld inzageverzoek 126

21 Bijlage 2: persoonsgegevens 129

22 Bijlage 3: MORA vergeleken met HORA 131

Voor deze verwerking relevante processen beschreven in HORA 132
Onderwijsplanning 132
Roosteren 133
Voor deze verwerking relevante processen beschreven in MORA 133
Plannen en Roosteren 133
Prognosticeren mensen- en middelen behoefte 136

Versiegeschiedenis

Versiegeschiedenis

Versie	Datum	Auteur(s)	Wijzigingen
1.0	8-7-2025	Sophia Gelpke, Jan Landsaat, Sue-Yin de Hoop	Eerste versie
1.7	17-9-2026	Sophia Gelpke, Jan Landsaat	Deel A en B herschreven n.a.v. wijzigingen bij Xedule, updates risico-inschattingen, nieuwe statustabel, nieuw risico toegevoegd
1.8	28-9-2026	Sophia Gelpke, Jan Landsaat	Feedback review Sanne Ouburg verwerkt
2.0	12-11-2026	Sophia Gelpke, Jan Landsaat	Feedback review Walter van Hest verwerkt, finale versie

Reviewgeschiedenis

Versie	Datum	Reviewer(s)	Notities
1.7	23-9-2026	Sanne Ouburg	Feedback over leesbaarheid, onjuistheden en tegenstrijdigheden
1.8	6-10-2026	Walter van Hest	Feedback over kloppendheid beschreven wijzigingen bij Xedule

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 onderzoeksinstellingen (hierna: instellingen), aangeboden door Xedule B.V. (voormalig Xedule Advitrae 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.

Deze versie van de DPIA is een update op versie 1.0 van de DPIA, gepubliceerd op 8 juli 2025 (hierna: de originele DPIA).

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. Na de originele DPIA heeft Xedule zijn verwerkersovereenkomst bijgewerkt. In de nieuwe versie zijn vier doeleinden waarvoor Xedule persoonsgegevens verwerkt als verwerker en vijf doeleinden waarvoor Xedule persoonsgegevens verwerkt als gemachtigd verwerkingsverantwoordelijke opgenomen.

Resultaat en conclusie: 10 risico's gemitigeerd naar laag, 6 overgebleven hoge risico's en 2 medium risico's, 1 nieuw laag risico

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

- 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.

Bij zeventien van deze risico's waren er maatregelen geïdentificeerd die Xedule moest treffen. Xedule heeft de maatregelen bij elf van deze zeventien risico's uitgevoerd, waardoor deze naar laag of medium zijn gebracht. Hiermee blijven er zes risico's over die instellingen niet zelf naar laag kunnen mitigeren. Xedule blijft werken om deze risico's te mitigeren en heeft nieuwe deadlines vastgesteld.

Voor het mitigeren van het overige, achttiende risico hoefden alleen de instellingen maatregelen te nemen. Daarnaast moesten de instellingen bij veertien van de risico's waarbij maatregelen voor Xedule waren vastgesteld zelf ook maatregelen treffen. Deze maatregelen blijven onverminderd van belang om de risico's naar laag te mitigeren.

Ook is er een nieuw, laag risico vastgesteld: Verlies van controle door verplichte openbaarmaking of onbevoegde toegang in derde landen.

Tabel 1-1 Update status risico's en maatregelen

Risico ***Dikgedrukt: instellingen moeten (ook) maatregelen nemen***	**Risico originele DPIA**	**Risico na update, mits instellingen ook maatregelen nemen**	**Maatregelen Xedule**	**Status maatregelen Xedule**
18.1 Verlies van controle door Xedule als verwerkingsverantwoordelijke	Hoog	Laag	Juridisch en feitelijk de rol van verwerker aannemen voor alle verwerkingen waarbij instellingen Xedule geen toestemming geven voor verdere verwerking als verwerkingsverantwoordelijke	Xedule heeft de verwerkersovereenkomst en het privacy statement bijgewerkt.

18.2 Verlies van controle door gebrek aan transparantie logging, pNPS en marketing	Hoog	Hoog	Inzage verschaffen in alle verwerkingen bij inzageverzoeken 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	Xedule heeft inzage gegeven in alle beschreven verwerkingen, heeft aangetoond toekomstige inzageverzoeken volledig en tijdig te kunnen beantwoorden en heeft het loggingbeleid bijgewerkt. Er is echter een discrepantie tussen het loggingbeleid en het inzageverzoek. Uiterlijk 31-12-2026 is het loggingbeleid aangepast en toepasbaar op de resultaten uit inzageverzoeken.
18.3 Verlies van vertrouwelijkheid en sociaal nadeel door te brede definiëring afwezigheids- en hulpmiddelencategorieën	Hoog	Hoog	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	Xedule heeft de interface van het definiëren van afwezigheidscategorieën aangepast, zodat deze gebruikers alert maakt op de impact van gevoelige categorieën. Uiterlijk 31-12-2026 breidt Xedule deze interface uit naar alle categorieënlijsten en voegt een waarschuwing toe door middel van een informatie-icoontje.
18.4 Niet mogelijk om AVG-rechten uit te oefenen en verlies van controle door gebrek aan transparantie subverwerkers	Hoog	Hoog	Hoofd- en verwerkersovereenkomst en sluiten met alle subverwerkers met een duidelijke instructie over de te verwerken persoonsgegevens en een lijst met subverwerkers	Xedule heeft SURF inzage gegeven in de overeenkomsten, maar deze sluiten niet aan bij de in deze DPIA vastgestelde rolverdeling tussen Xedule als verwerker en de instellingen als verwerkingsverantwoordelijke. Uiterlijk 31-1-2027 werkt Xedule de contracten bij.

18.5 Verlies van vertrouwelijkheid door doorgeven beschikbaarheidsredenen aan roosteraars	Hoog	Medium	Mogelijkheid implementeren om beschikbaarheidsredenen te verbergen voor gebruikers die er geen toegang toe nodig hebben voor hun functie Duidelijke strategie implementeren om klanten en gebruikers (in de context van de verwerking) te waarschuwen geen (bijzondere) persoonsgegevens in open velden op te nemen	Xedule heeft de applicatie aangepast, zodat instellingen de mogelijkheid hebben om de beschikbaarheidswijziging in zijn geheel niet door te geven aan roostermakers. Als deze functionaliteit wel aanstaat, worden gebruikers gewaarschuwd dat de informatie die ze in het opmerkingenveld opnemen wordt gedeeld met de roostermaker. Uiterlijk 31-12-2026 zal Xedule zorgen dat het doorgeven verder beperkt wordt, maar wel zichtbaar gehouden voor de teamleider.
18.6 Verlies van controle en vertrouwelijkheid door overige vrije velden	Hoog	Laag	Duidelijke strategie implementeren om klanten en gebruikers (in de context van de verwerking) te waarschuwen geen (bijzondere) persoonsgegevens in open velden op te nemen	Xedule heeft een waarschuwingstekst via een informatie-icoon geplaatst.
18.7 Gemiste kansen en verlies van vertrouwelijkheid door handmatige invoer	Medium	Medium*	-	Geen maatregelen voor Xedule
18.8 Verlies van controle en vertrouwelijkheid door niet automatisch te configureren bewaartermijnen	Hoog	Laag	Technische configuratie en beheer van bewaartermijnen per groep persoonsgegevens faciliteren Inzichtelijk maken procedure verwijderen persoonsgegevens door middel van een verzoek aan Xedule	Xedule heeft automatische bewaartermijnen ingesteld per ORE. Alle gegevens die niet aan een ORE gekoppeld zijn, waaronder verzuim- en verlofgegevens, moeten handmatig worden verwijderd. Daarnaast heeft Xedule inzage gegeven in de manier waarop functioneel

				beheerders Xedule handmatig persoonsgegevens kan laten verwijderen. NB Voor verdere ontwikkeling van functionaliteiten om bewaartermijnen automatisch te configureren heeft Xedule input over de behoeftes van instellingen nodig.
18.9 Niet uit kunnen oefenen van AVG-rechten door incomplete inzageverzoeken	Hoog	Laag	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	Xedule heeft inzage gegeven in alle beschreven verwerkingen en heeft aangetoond toekomstige inzageverzoeken volledig en tijdig te kunnen beantwoorden.
18.10 Verlies van controle en vertrouwelijkheid door het niet hebben van automatische import/export	Hoog	Laag	Optie van automatische import/export uitlichten en aanraden waar mogelijk Automatische import/export faciliteren waar mogelijk	Xedule wijst instellingen via de online help op de mogelijkheid van automatische import/export en gebruikt een csv-template met invoervalidatie.
18.11 Verlies van controle en vertrouwelijkheid door tabellen	Hoog	Hoog	Configuratiemogelijkheden bieden om de optie om gegevens uit tabellen te kopiëren en exporteren gericht uit te schakelen	Uiterlijk 31-12-2026 stelt Xedule een functionaliteit beschikbaar waarmee het kopiëren van tabellen buiten de desktopapplicatie onmogelijkheid gemaakt kan worden en gebruikers een waarschuwing krijgen als ze tabellen proberen te kopiëren buiten de webapplicatie.

18.12 Verlies van vertrouwelijkheid door handmatige RBAC	Hoog	Laag	Ondersteun een geautomatiseerde koppeling met externe identiteits- en toegangsbeheersystemen	Xedule stelt een geautomatiseerde koppeling beschikbaar aan iedere instelling die hierom vraagt.
18.13 Verlies van vertrouwelijkheid door onduidelijke configuratiewijzigingen	Hoog	Hoog	Richt de interface op een manier die onbewuste autorisatiefouten tegengaat, bijvoorbeeld door visueel duidelijk te maken voor gebruikers welke autorisatiewijzigingen er zijn doorgevoerd	Uiterlijk 31-3-2027 voert Xedule deze wijziging door.
18.14 Verlies van vertrouwelijkheid door Xedule rest API	Hoog	Laag*	Wijzig het autorisatiemodel van de API, zodat de toegang door een ander systeem tot een dataset beperkt kan worden tot de minimaal benodigde set	Xedule stelt het Connect platform beschikbaar*, waarmee verschillende koppelingen verschillende API keys krijgen.
18.15 Verlies van vertrouwelijkheid en controle door ongeautoriseerde toegang door verouderde SOAP API	Hoog	Laag	Ondersteuning van de SOAP API uitfaseren	Xedule heeft instellingen geïnformeerd over de mogelijkheid over te stappen naar een andere API.
18.16 Heridentificering van gepseudonimiseerde gegevens door gebrekkige anonimiseringsmethode	Hoog	Laag	In de dienstverlening duidelijk maken dat het om pseudonimisering gaat	Xedule heeft de privacyverklaring en andere documentatie aangepast, zodat het duidelijk is dat de aangeboden dienstverlening pseudonimisering betreft.
18.17 Heridentificering gepseudonimiseerde pNPS-gegevens	Hoog	Hoog	Verander het mechanisme naar opt-in Implementeer aantoonbare maatregelen om heridentificatie te voorkomen	Xedule biedt instellingen nu de actieve keuze om pNPS-uitvragen in de applicatie toe te staan. NB Het invullen van deze uitvragen kan ertoe leiden dat Xedule contact opneemt met de instelling voor opvolging. Instellingen moeten ervoor zorgen dat

				medewerkers hiervan op de hoogte zijn, aangezien de medewerkers identificeerbaar zijn op basis van hun reacties op de uitvragen. Uiterlijk 31-12-2026 verwijdert Xedule het user ID uit Survicate, zodat heridentificatie moeilijker wordt. Ook verwijdert Xedule opmerkingen voordat de score wordt doorgegeven aan BigQuery.
18.18 Verlies van vertrouwelijkheid door door ontbreken 'read access logging'	Hoog	Laag	Read access logging implementeren	Xedule heeft volledige inzage gegeven de read access logging en heeft aangetoond toekomstige inzageverzoeken volledig en tijdig te kunnen beantwoorden.
NIEUW 18.19 Verlies van controle door verplichte openbaarmaking of onbevoegde toegang in derde landen	-	Laag	(Een periodieke beoordeling van de geopolitieke situatie om vast te stellen of de risicobeoordeling moet worden aangepast en een alternatief doorgiftemechanisme moet worden ingezet.)	

* De maatregel is een betaalde optie.

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 Noodzaak DPIA

Instellingen kunnen als verwerkingsverantwoordelijken de wettelijke verplichting hebben om een gegevensbeschermingeffectenbeoordeling ofwel een Data Protection Impact Assessment (hierna: DPIA) uit te voeren. Aangezien instellingen Xedule inschakelen als verwerker, hebben zij deze verplichting ten opzichte van verwerkingen in Xedule die voldoen aan de vereisten voor een DPIA. 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 lijst[1] opgesteld van soorten verwerkingen waarvoor het uitvoeren van een DPIA verplicht is. Ook de EDPB[2] heeft een lijst opgesteld met negen criteria die kunnen bepalen of een verwerking een verhoogd

[1] Autoriteit Persoonsgegevens, *Data protection impact assessment (DPIA)*, 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.

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.

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 SURF[3] 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.

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

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 onderzoeksinstellingen. 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

[3] SURF, *Overzicht leden van SURF,* https://www.surf.nl/over/overzicht-leden-van-surf, geraadpleegd op 8 september 2026.

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 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 genomen 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 3.0.[5] Dit model sluit goed aan op de werkzaamheden van onderwijs- en onderzoeksinstellingen, die ze onder andere 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.

[4] Zie ook: Sectorbeeld Onderwijs 2021-2023, 24 January 2024, p. 5-6, https://www.autoriteitpersoonsgegevens.nl/documenten/sectorbeeld-onderwijs-2021-2023.

[5] CIP, *Model DPIA Rijksdienst,* https://www.cip-overheid.nl/producten-en-diensten/de-8216-rijkspia-8217, geraadpleegd op 9 september 2026.

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 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

De scope van deze DPIA omvat en beperkt zich 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

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 aantal[6] mbo- en hbo-instellingen maakt gebruik van Xedule en My Xedule. 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 Xedule en Visma

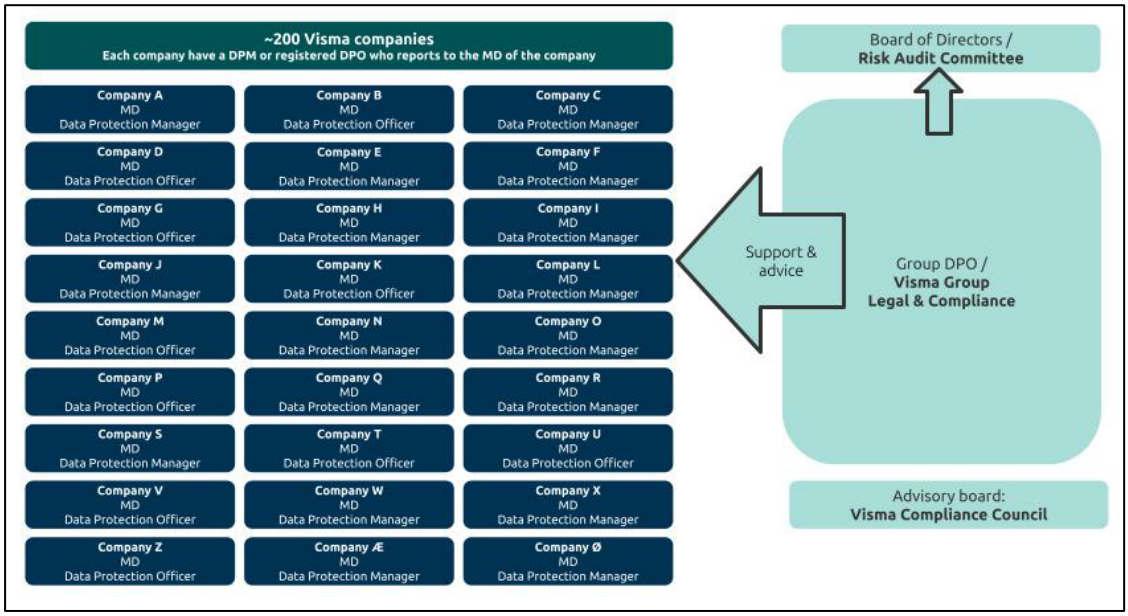
Xedule maakt deel uit van de Visma Group (Visma Software International AS, hierna: Visma Group of Visma AS). De Visma Group is het Europese moederbedrijf van ruim 200 Xedule dochterondernemingen, waaronder Xedule B.V. De Visma Group heeft een overkoepelende strategische rol en algemene kaders en richtlijnen 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 Group.[7] 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

[6] Gebruikersgroep Xedule, https://mbodigitaal.nl/activiteiten/gebruikersgroepen/gebruikersgroep-xedule/, geraadpleegd op 11 november 2026.

[7] Our approach to privacy, https://www.visma.com/trust-centre/privacy, geraadpleegd op 11 november 2026.

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.

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

3.2 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. Het zijn beiden webapplicaties die Xedule aanbiedt als Software-as-a-Service (SaaS). 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.

3.2.1 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.

3.2.2 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 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 selfserviceplatform 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.

3.2.3 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 5 Persoonsgegevens.

Voor het maken en het tonen van roosters in My Xedule worden applicaties met onderwijslogistieke gegevens (hierna: bronsystemen), 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.

4 Verwerkingsdoeleinden

Xedule verwerkt persoonsgegevens van studenten en medewerkers van instellingen voor verschillende doeleinden. De hoofddoelen waarvoor instellingen Xedule gebruiken zijn onderwijsplanning en roostering. Deze overkoepelende doeleinden zijn in paragraaf 4.1 Hoofddoelen instellingen (conform HORA) 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. Deze doeleinden zijn vastgelegd in de verwerkersovereenkomst, zoals besproken in paragraaf 4.2 Verwerkingsdoeleinden instellingen verwerkersovereenkomst. Verder is er een uitputtende lijst doeleinden in de verwerkersovereenkomst vastgelegd waarvoor Xedule als gemachtigd verwerkingsverantwoordelijke persoonsgegevens mag verwerken, zoals besproken in paragraaf 4.3 Verwerkingsdoeleinden Xedule verwerkersovereenkomst.

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 Hoofddoelen 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 instellingen: Onderwijsplanning

Instellingen gebruiken Xedule voor de volgende doelen op het gebied van het 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.

[8] Bedrijfsfunctiemodel (detail), https://hora.surf.nl/index.php/Bedrijfsfunctiemodel_(detail), geraadpleegd op 11 november 2026.

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

- **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.

- **Vraagprognotisering:**

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 geprognotiseerde 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.

4.1.2 Hoofddoel instellingen: Roostering

Instellingen gebruiken Xedule voor de volgende doelen op het gebied van het 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 Verwerkingsdoeleinden instellingen verwerkersovereenkomst

De doeleinden waarvoor Xedule als verwerker gegevens moet verwerken ten behoeve van de instellingen, zodat de instellingen hun hoofddoelen kunnen uitvoeren, zijn als volgt vastgelegd in de verwerkersovereenkomst:

i) Beschikbaar stellen van de applicaties
ii) Bieden van ondersteuning aan de onderwijsinstelling
iii) Beveiliging van (persoons)gegevens die in de applicaties zijn opgenomen
iv) Technische verbeteringen van de applicatie zoals bugfixes, patchmanagement en onderhoud

In de bijlage is een specificatie opgenomen van de precieze verwerkingsactiviteiten die ten behoeve van deze doelen worden uitgevoerd, die in lijn is met deze DPIA, specifiek hoofdstuk 6 Gegevensverwerkingen.

4.3 Verwerkingsdoeleinden Xedule verwerkersovereenkomst

Daarnaast moet Xedule persoonsgegevens verwerken voor een aantal eigen, legitieme zakelijke doeleinden als gemachtigd verwerkingsverantwoordelijke (zie paragraaf 7.3 Xedule: Gemachtigd verwerkingsverantwoordelijke). Deze doeleinden zijn:

1. Gebruiken van contactgegevens van medewerkers van de onderwijsinstelling die het functionele beheer van de applicaties verzorgen ten behoeve van:
    - Het efficiënt en effectief gebruiken van de applicaties
    - Serviceberichten zoals patchnotes, releasenotes en statusberichten
    - Bieden van ondersteuning bij vraagstukken
2. Gebruiken van contactgegevens van medewerkers van de onderwijsinstelling die betrokken zijn bij de dienstverlening ten behoeve van:
    - Contractuele verplichtingen zoals verlengingen, aanbestedingen, marktconsultaties, facturatie en inzet van medewerkers van Verwerker ter ondersteuning van de onderwijsinstelling
    - Verbeteringen en nieuwe functionaliteiten die buiten de dienstverlening vallen die in de bovenliggende overeenkomst opgenomen zijn
    - Onderwijslogistieke kennisoverdracht, innovatie en branchegerelateerde onderwerpen
3. Verzamelen van gegevens om te voldoen aan wettelijke verplichtingen, zoals het opvolgen van verzoeken tot verplichte verstrekking van persoonsgegevens vanuit autoriteiten en toepasselijke wetgeving met inachtneming van de overeengekomen voorwaarden in artikel 5.

4. Verzamelen van technische gegevens om noodzakelijke verandertrajecten in technische componenten van de applicaties te faciliteren.
5. *OPTIONEEL: keuze acceptatie bij verwerkingsverantwoordelijke* Verzamelen van gepseudonimiseerde scores en persoonsgegevens uit opmerkingenvelden bij functioneel beheerders, deze combineren met andere gegevens, ook van andere organisaties, deze aggregeren en contact opnemen met verwerkingsverantwoordelijke naar aanleiding van deze informatie teneinde de applicaties te verbeteren met inzichten van gebruikers.

Xedule mag deze lijst niet eenzijdig uitbreiden en voert verwerkingen voor deze doeleinden uitsluitend uit wanneer ze strikt noodzakelijk en evenredig zijn.

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 identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;"*

Xedule sluit met de terminologie in haar Privacy Statement 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."[10]

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.

[10] Privacy Statement Xedule B.V., 16 oktober 2026.

Afhankelijk van de wensen van de onderwijsinstelling, kunnen verschillende bronsystemen worden gekoppeld aan Xedule. Welke persoonsgegevens er uiteindelijk uit deze 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 Xedue 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 bronsystemen[11], 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 Middelenplanning) 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.

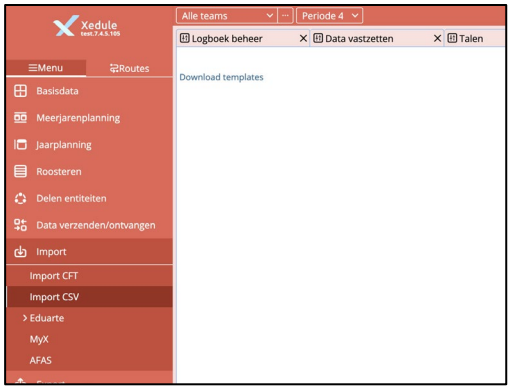
De locatiegegevens worden eenmalig gebruikt om de bevestiging van de faciliteit te organiseren. Deze worden niet opgeslagen in het systeem.

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.

Sinds najaar 2025 heeft Xedule het gebruik van een template bij het importeren van data verplicht gesteld. Deze templates worden via de interface als download aangeboden.



Figuur 5-1, de templates worden via de interface van Xedule aangeboden.

6.1.2.2 Handmatige invoer

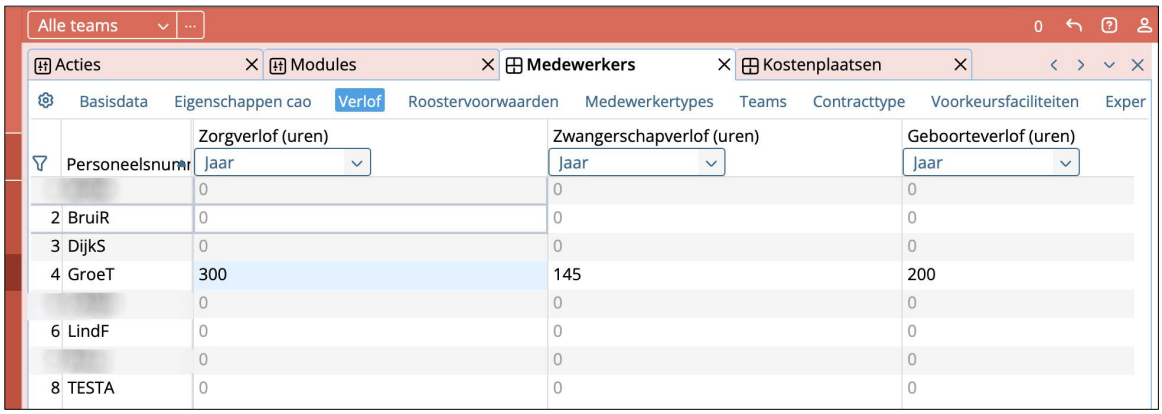
Roosteraars en/of functioneel beheerders kunnen handmatig persoonsgegevens invoeren en bewerken in Xedule. Deze handmatige verwerking vindt plaats via directe invoer in het systeem, waarbij nieuwe gegevens kunnen worden toegevoegd en bestaande gegevens kunnen worden gewijzigd of verrijkt. Denk hierbij 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.

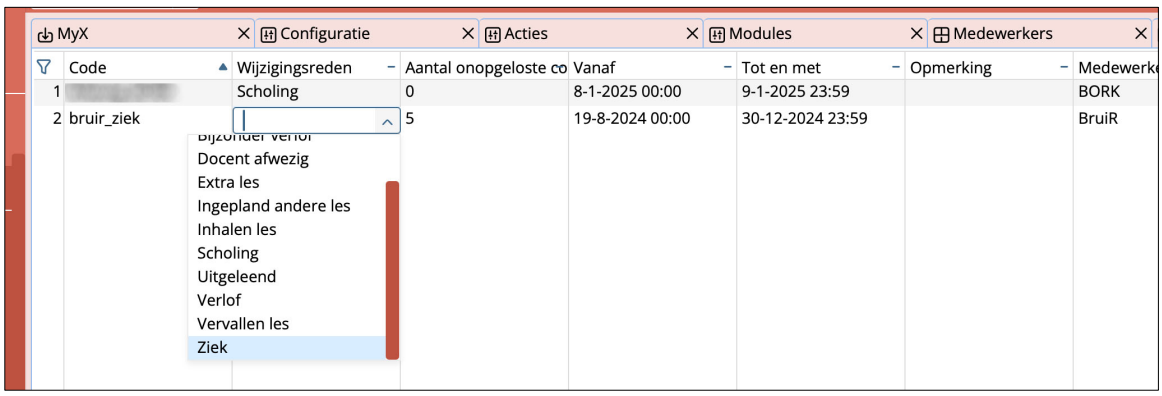
Verlofgegevens: Voor het ondersteunen van Onderwijsplanning kunnen verlofgegevens van medewerkers in Xedule worden verwerkt, waaronder bijzondere persoonsgegevens, zoals zwangerschapsverlof. Deze persoonsgegevens kunnen zowel door de roosteraar handmatig

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.



Figuur 5-2, Invoeren verlofgegevens.

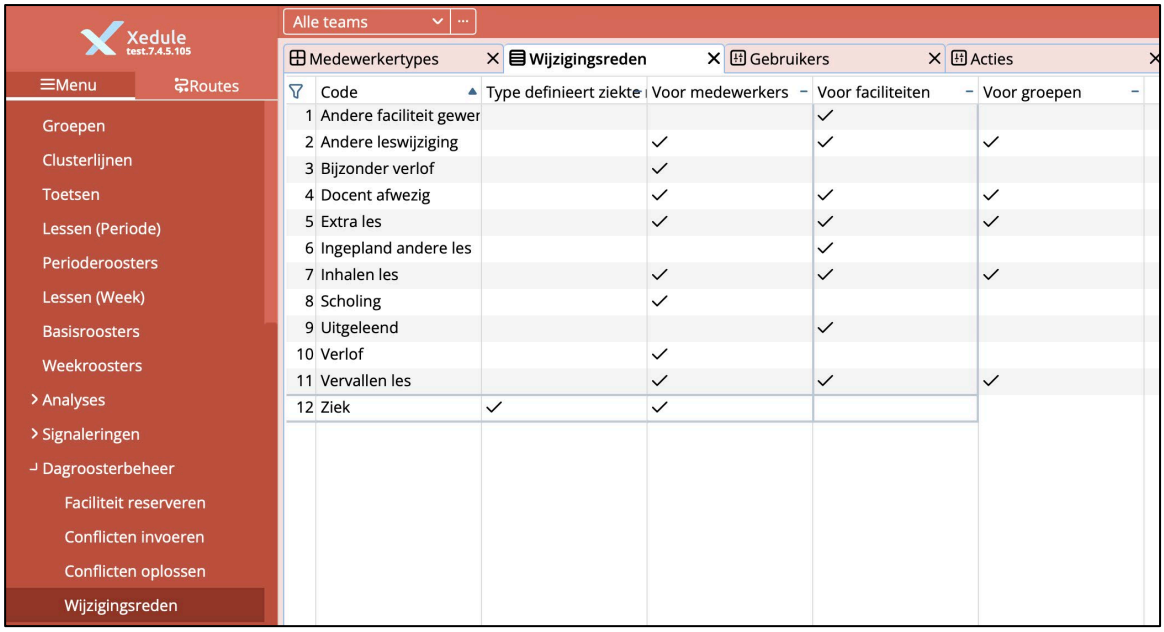
Afhandelen afwezigheidsmeldingen: Een belangrijke functionaliteit van Xedule is dagroosterbeheer. Dagroosterbeheer richt zich op het oplossen van last-minute roosterconflicten. Tijdens dit proces kunnen de roosteraars de reden van het roosterconflict registreren, denk bijvoorbeeld aan afwezigheid van 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.



Figuur 5-3, 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.

Update najaar 2026
Sinds najaar 2025 heeft Xedule de interface rond het beheer van de afwezigheidslabels aangepast zodat de autorisatie tot deze labels te beheren is. Deze wijziging zorgt ervoor dat tijdens het beheer van deze labels er verplicht keuzes gemaakt moeten worden die meer duidelijkheid geven in de inzage en gevoeligheid van deze labels.



Figuur 5-4, de aangepaste interface ‘wijzigingsredenen’.

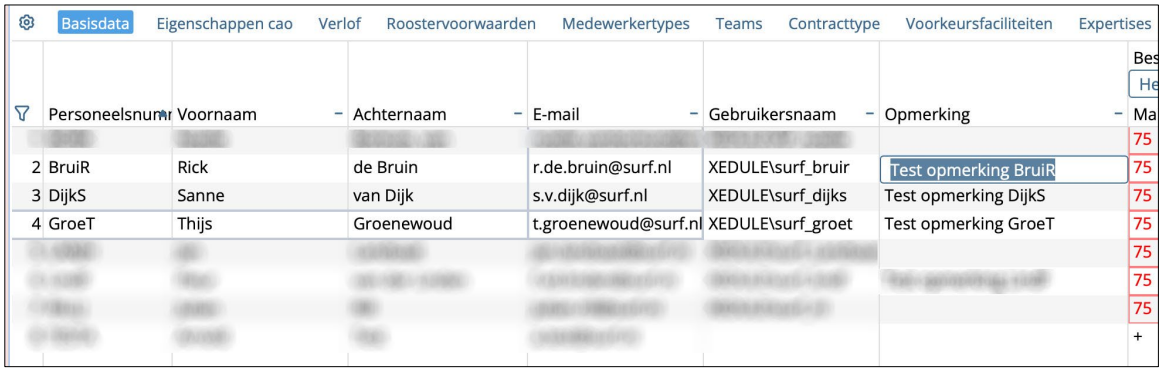
Meer in hoofdstuk 18.3 Verlies van vertrouwelijkheid en sociaal nadeel door te brede definiëring afwezigheids- en hulpmiddelencategorieën.

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 picklist[12] 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

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

onderwijsinstelling vrij om hier invulling aan te geven. Deze zijn voor de daartoe gemachtigde gebruikers zichtbaar.



Figuur 5-5, Vrij veld bij een gebruiker.

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 5-6). De link in de disclaimer leidde in de testomgeving naar een specifieke privacyverklaring (zie Figuur 5-8).

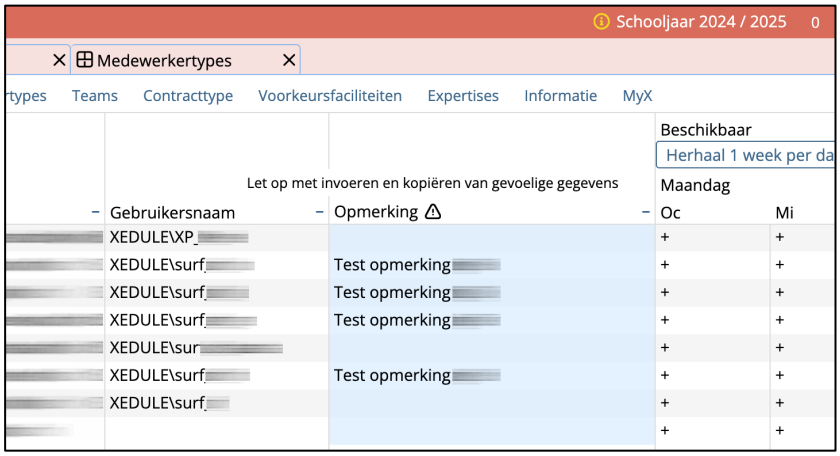


Figuur 5-6, disclaimer rond vrije invulvelden.



Figuur 5-7, Tekst over vrije invulvelden.

Sinds najaar 2025 heeft Xedule de open velden in Xedule (vrije comment velden) voorzien van een icoon (!) wat ‘on hover’ een waarschuwing weergeeft: “Dit is een vrij tekstveld. Vul hier uitsluitend noodzakelijke en functionele informatie in conform het beleid van je onderwijsinstelling.” Deze tekst wordt ter verduidelijking bijgewerkt naar: "Voer geen bijzondere en gevoelige persoonsgegevens in, tenzij dit volgens je instellingsbeleid mag."



Figuur 5-8, het uitroepteken met de waarschuwing.

Meer hierover in hoofdstuk 18.6 Verlies van controle en vertrouwelijkheid door overige vrije velden.

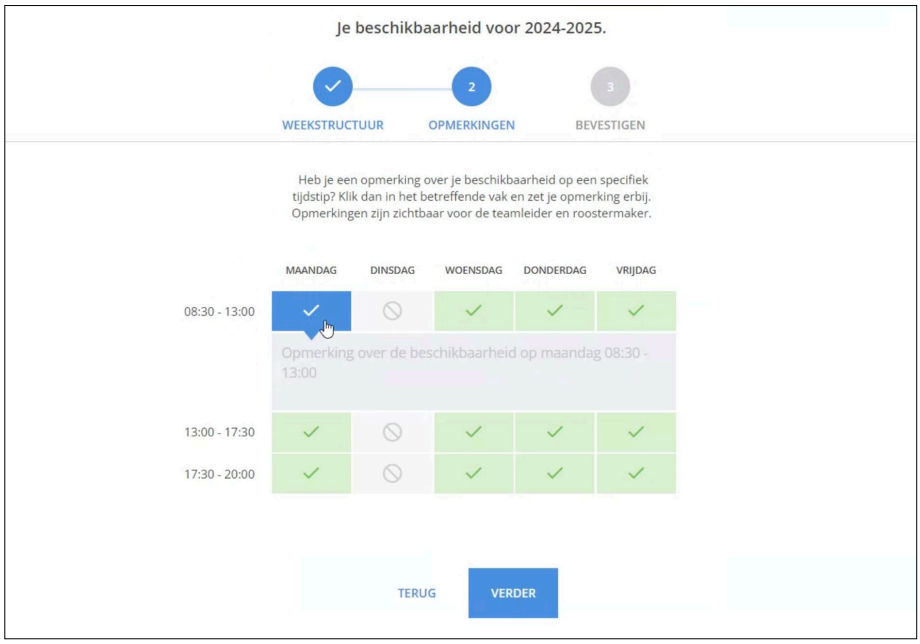
6.1.2.5 |*My Xedule*| *Beschikbaarheid*

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 is er de optie voor de verwerkingsverantwoordelijke om een tekstveld ter motivatie (comment) aan te zetten. Het is zeer aannemelijk dat er gevoelige of zelfs bijzondere persoonsgegevens in dit motivatieveld worden verwerkt. Het motivatieveld staat standaard uit voor nieuwe klanten van Xedule en bestaande klanten kunnen het uit zetten via het configuratiescherm in Xedule (zie Figuur 5-10).

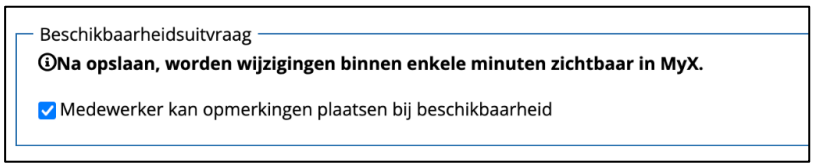
Als deze motivatieveld funcie aan staat wordt de inhoud gedeeld met de leidinggevende welke dan deze motivatie mee kan nemen als context om de beschikbaarheids aanvraag te fiatteren. Als deze is goedgekeurd wordt deze inclusief motivatie doorgezet naar de roosteraar. Voor de betrokkene is het veld voor doorgeven van beschikbaarheid voorzien van uitleg, wie er inzage heeft in de motivatie (zie Figuur 5-11).

Tijdens het onderzoek voor de originele DPIA (1.0) stond deze functionaliteit standaard aan en was het niet mogelijk om uit te zetten (Figuur 5-9).

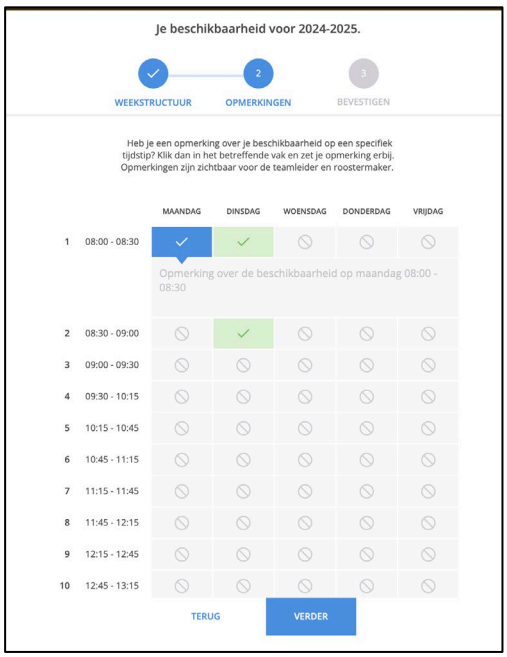
Meer in hoofdstuk 18.5 Verlies van vertrouwelijkheid door doorgeven beschikbaarheidsredenen aan roosteraars.



Figuur 5-9, het originele vrij invulveld bij doorgeven beschikbaarheid, DPIA 1.0.



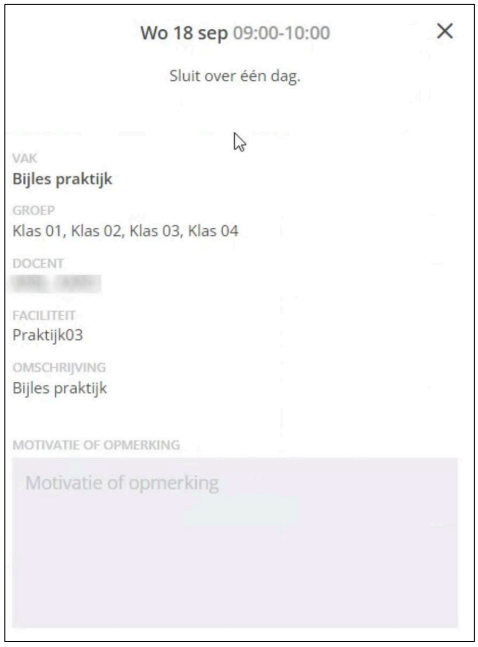
Figuur 5-10, de optie om de mogelijkheid tot motivatie aan/uit te zetten.



Figuur 5-11, de uitleg over wie toegang heeft tot de motivatie.

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).



Figuur 5-12, 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 hostingpartij 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

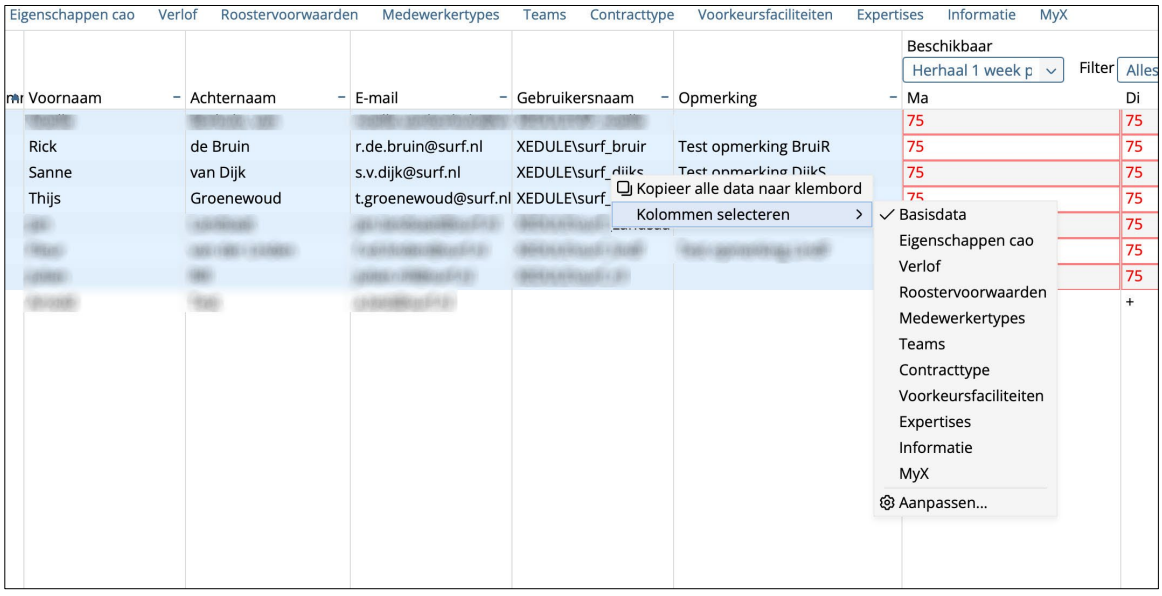
personen aan elkaar te koppelen. Roosteraars en functioneel beheerders kunnen, afhankelijk van hun autorisatie, via Xedule de al ingelezen contentdata wijzigen en/of bijwerken. Zoals eerder is benoemd, is de accountdata in Xedule een kopie van de persoonsgegevens (stamgegevens) uit het bronsysteem wat 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.

In het najaar van 2026 is er intern een wijzigingsverzoek door de compliance-afdeling van Xedule gedaan. In dit verzoek worden de twee versies van Xedule voorzien van technische maatregelen.

1. De desktopapplicatie krijgt de beperking dat alle vanuit Xedule gekopieerde data alleen geplakt kan worden binnen Xedule.
2. De webversie krijgt één mededeling/notificatie/waarschuwing per sessie wanneer er gekopieerd wordt waarin verzocht wordt om aan de protocollen van de instelling te houden bij kopiëren en plakken.

Meer in hoofdstuk 18.11 Verlies van controle en vertrouwelijkheid door tabellen.



Figuur 5-13, kopieren 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 faciliteitreserveringen. 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) gekoppled 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 was tijdens het onderzoek van de originele DPIA (1.0) voor een onderwijsinstelling op drie manieren mogelijk om persoonsgegevens te verwijderen. In voorjaar 2026 is daar een vierde optie bij gekomen.

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.
4. Definiëren van bewaartermijnen binnen een ORE.

Definiëren bewaartermijnen binnen een ORE
Instellingen kunnen per ORE bewaartermijnen definiëren voor medewerkersdata, studentdata en opmerkingen & omschrijvingen. De termijnen gaan in waarden van 1 tot en met 10 in jaren.

Medewerkersdata bestaat uit: Voornaam, achternaam, login/gebruikersnaam, e-mail, opmerking, personeelsnummer en opmerkingen op tijdigheidskolommen (Studeert en Beschikbaar).

Studentdata bestaat uit: Voornaam, achternaam, login/gebruikersnaam, e-mail, opmerking, studentnummer en opmerkingen op tijdigheidskolommen (Studeert en Beschikbaar).

Opmerkingen & omschrijven bestaat uit: Kolommen 'Opmerking' en/of 'Omschrijving' en opmerkingen op alle tijdigheidskolommen.

Rekenvoorbeeld vanuit documentatie Xedule[13]
Huidige datum: 21 mei 2026
Ingestelde termijn: 2 jaar
Bewaartermijn datum: 21 mei 2024 (dit valt binnen schooljaar 23/24)
Effect: Alle data uit schooljaren ouder dan schooljaar 23/24 worden geanonimiseerd.

De datum waarop je de bewaartermijn invoert is ook het moment dat de 'teller' gaat lopen. Dus 'x' jaar na instellen van bewaartermijn op een ORE worden de gegevens binnen dat schooljaar geanonimiseerd. Xedule anonimiseert deze 'datapoints' door de gegevens te overschrijven met generieke gegevens, bijvoorbeeld "Flip Flippenstein" wordt "naam student".

Xedule heeft aangegeven dat het deze dienst blijft evalueren nu instellingen daar actief gebruik van gaan maken, zodat deze service aangepast kan worden naar de daadwerkelijke wens.

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.

[13] Bewaartermijnen instellen voor privacygevoelige data, https://support.xedule.nl/hc/nl/articles/36237385246738-Beheer-Configuratie-Databeheer, geraadpleegd op 19 oktober 2026.

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 roosteraar[14].

Wanneer een actie aan een gebruikersrol toegekend wordt, zal een rechtenniveau gedefinieerd moeten worden voor die actie. Xedule maakt onderscheid tussen beheer-, schrijf- en leesrechten[15]:

- 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

[14] Xedule Help \ Beheer \ Autorisatie \ Gebruikersgroepen.

[15] Xedule Help \ Beheer \ Autorisatie \ Acties.

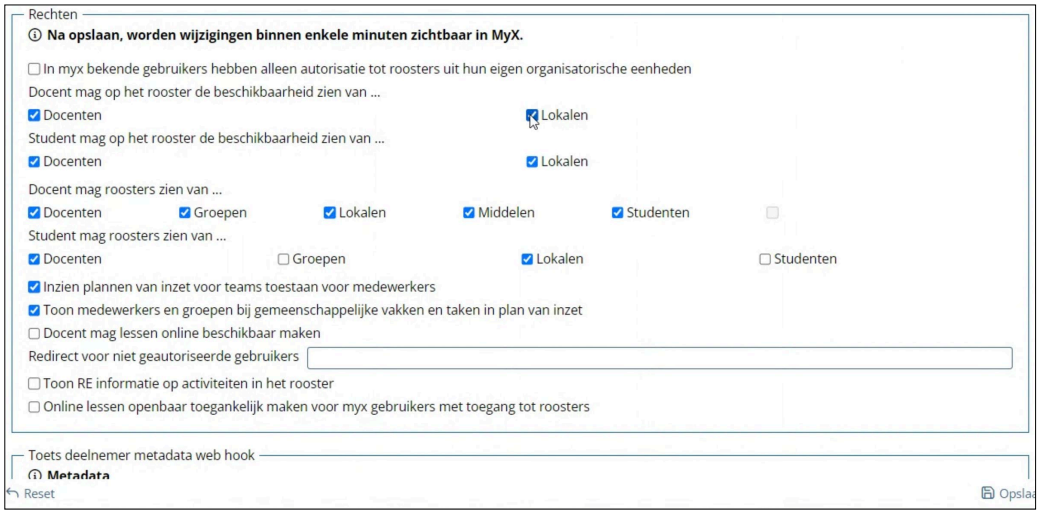
rollen. Hierdoor is het mogelijk om de toegang tot gegevens te regelen en aan te passen aan de eigen beleidskeuzes.

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).

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).



Figuur 5-14, screenshot systeeminstellingenscherm 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).

Xedule heeft het loggingbeleid 1.0 (februari 2025) gedeeld met SURF. SURF heeft deel A van de originele DPIA op basis hiervan geschreven.

Tijdens de update op de DPIA (zomer 2026) heeft Xedule het loggingbeleid aangescherpt naar versie 2.0 (oktober 2026) naar aanleiding van de maatregelen in de originele DPIA door SURF waren vastgesteld. Zie ook paragraaf 18.2 Verlies van controle door gebrek aan transparantie logging, pNPS en marketing.

Dit herziene logbeleid[16] geeft het volgende overzicht van de logpraktijken door Xedule.

Logbron	Vast te leggen gebeurtenissen	Verplichte velden & Details	Reden van vastleggen
Firewall	Toegestane en geblokkeerde netwerkverbindingen naar de applicatieserver.	Bron-IP, Bestemmings-IP, Poort, Protocol, Tijdstempel, Actie (Allow/Deny).	Netwerkbeveiliging, bescherming tegen DDoS, toegang beperken en storingsanalyse.
Microsoft Entra ID (Azure AD)	Authenticatiepogingen, token-uitgifte, MFA-resultaten, afwijkende inlogpogingen.	User Principal Name (UPN), Tenant ID, IP-adres, Client App, Session ID, Correlation ID.	Identiteitsbeheer, herleidbaarheid van aanmeldingen en opsporen van ongeoorloofde toegang.
IIS Web Server	Alle inkomende HTTP GET-/READ-verzoeken op de webserver.	Datum/Tijd (UTC), Client IP (c-ip), Method (GET), URI Stem (cs-method), Status Code, Response Size, Time-Taken (ms).	Toegangscontrole op URL-niveau en analyse van webservertoegang.
Front-Office (FO)	Gebruikersnavigatie, schermopvragingen, geopende tabs en client-side time-outs.	Gebruikersnaam, Frontend Session ID, Scherm/Tab naam, Application Version, Log Level (INFO, WARN, FATAL).	Inzicht in functioneel gebruik, herleidbaarheid van schermacties en troubleshooting.
Data Access Layer (DAL)	Directe query's op stamdata, scenario-opvragingen, datagrid-views en data-fetches.	Gebruikersnaam, Dataset/Scenario ID, Opgevraagde Entiteit (bijv. Medewerkers, Logs), Parameters, Record Counts.	Gedetailleerd inzicht bij gegevensinzage, datalekken, misbruik en foutief gebruik.
Azure Application Insights*	End-to-end tracing, kartering van afhankelijkheden en applicatiefouten (exceptions). Vastlegging van persoonsgegevens wordt toegepast bij foutmeldingen	Operation_Id, Parent_Id, Exception Message, Request Latency, Dependency Calls.	Monitoring van prestaties, beschikbaarheid en diepgaande foutdiagnose.

Tabel 6-1, overzicht van loggingpraktijken zoals vermeld in logging beleid van Xedule sinds zomer 2026.

Het logbeleid bevat enkele algemene begrippen die tot onduidelijkheid leiden over wat er exact vastgelegd wordt. Zo laten de datasets achter ‘end-to-end tracing’ en ‘kartering van afhankelijkheden’ een ruime interpretatie toe. Als we het logbeleid naast de resultaten van

[16] Xedule Logging Beleid | 2026 Logging beleid.pdf

het inzageverzoek (zie paragraaf 6.4.2 Inzageverzoeken zomer 2026) leggen blijken deze gegevens te ontbreken. Waar in de oorspronkelijke DPIA (zie paragraaf 6.3.1 Microsoft Azure Application Insights) nog wel dataverkeer met betrekking tot deze verwerkingen werd vastgesteld, was dit bij het onderzoek horend bij de update niet het geval. Dit roept vragen op over de consistentie van wat er op welk moment wordt gelogd, en wekt de indruk dat er gegevens missen in de reactie op het inzageverzoek.

Autorisatie
Toegang tot logbestanden is beperkt tot geautoriseerde systeembeheerders en geautoriseerde medewerkers van Xedule support. Logs bevinden zich op een afgeschermde locatie en zijn niet aan te passen. Bij een inzageverzoek worden geschoonde logs aan de instelling verstrekt waar privacy- of securitygevoelige informatie (van anderen) uit is gehaald. Als er reden is voor forensisch onderzoek, worden de logs veiliggesteld op een afgeschermde plek waar alleen de Information Security Manager van Xedule toegang tot heeft.

Persoonsgegevens (user-id, IP-adressen) zijn in dashboards die Xedules support inziet afgeschermd of gepseudonimiseerd. Alleen bij geautoriseerde forensische onderzoeken worden de ruwe logbestanden gebruikt.

Encryptie
Logdata is zowel in rust (at rest, bijv. AES-256) als tijdens transport (in transit, TLS 1.2/1.3) versleuteld.

Bewaartermijnen

Firewall:	6 maanden (180 dagen)
IIS Web Server Logs:	6 maanden (180 dagen)
Entra ID:	1 jaar (365 dagen)
Authenticatie Logs:	1 jaar (365 dagen)
Front-Office (FO):	1 jaar (365 dagen)
DAL Access Audit Logs:	1 jaar (365 dagen)
Azure Application Insights:	90 dagen

6.3.1 Microsoft Azure Application Insights
Om van stabiliteit en functionaliteit van de applicaties te monitoren, technische problemen vroegtijdig te identificeren en de gebruikerservaring te verbeteren maakt Xedule gebruik van Microsoft Azure Insights. 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 "*End-to-end tracing, kartering van afhankelijkheden en applicatiefouten (exceptions). Vastlegging van persoonsgegevens wordt toegepast bij foutmeldingen.*"

Vanuit de technische analyse horend bij de originele DPIA (zie bijlage 19.1 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 toen of hierbij of het IP-adres van de betrokkene ook wordt verwerkt.

Xedule heeft toen 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 op twee momenten inzageverzoeken (DSARs) ingediend bij Xedule, tijdens het originele onderzoek in najaar 2024 en tijdens het update onderzoek van zomer 2026.

6.4.1 Inzageverzoeken najaar 2024

De inzageverzoeken gekoppeld aan het originele onderzoek waren naar aanleiding van de verschillende scenario's (zie 19.2 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:
Verstrekte 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 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.

6.4.2 Inzageverzoeken zomer 2026

De inzageverzoeken gekoppeld aan het updateonderzoek van zomer 2026 waren naar aanleiding van de wijzigingen die Xedule heeft doorgevoerd in Xedule en MyXedule. Dit betreft dus niet een geheel technisch onderzoek en daarmee ook een kleiner inzageverzoek. Voor meer zie 20.3 Testscenario’s zomer 2026.

De ontvangen datasets naar aanleiding van de inzageverzoeken kwamen binnen de termijn van 30 dagen binnen en waren volledig, met uitzondering van de logs van Azure Insights, Firewall logs en de Read Access Logs. De Azure Insights-logs ontbraken in de reactie, terwijl de Read Access Logs lieten zien waar de gebruiker in Xedule was geweest, maar geen duidelijkheid boden over welke data werd ontsloten (filter- en zoekquery’s ontbreken). Xedule is naar aanleiding van deze omissie een onderzoek gestart.

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 besluitvorming[17]

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 Backup[18]

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 locaties[19], 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 Objective[20] = < 2 uur, Recovery Time Objective [21]= < 12 uur;
- Databases met klantdata worden dagelijks veiliggesteld. Recovery Point Objective = < 2 uur, Recovery Time Objective = < 12 uur;

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

[18] 240130 Backup en restore document versie 1.3.pdf.

[19] Hostingpartij Interconnect zie hoofdstuk 8.4 Subverwerkers van Xedule.

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

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

7.4 Pseudonimiseren

Xedule pseudonimiseert de verzamelde feedback data (customer satisfaction score) via Product Net Promoter Score (pNPS) sinds voorjaar 2026 via Survicate (zie ook 8.3.1 Verbeteren van dienstverlening en applicatie). Deze feedback wordt enkel gevraagd aan personen die toegang hebben tot Xedule (admins, roosteraars, proces managers). Studenten en docenten worden niet blootgesteld aan deze verwerking. Eind 2025 heeft Xedule de instellingen gevraagd of ze (nog) gebruik van pNPS willen maken. Voor nieuwe klanten wordt er tijdens het implementatie proces stilgestaan of de instelling hier gebruik van wil maken. Gebruikers zijn niet verplicht om feedback te geven en kunnen de feedback vraag zonder gevolgen wegklikken.

De uitvraag is een vraag met een score en een eventuele motivatie van deze score.



Figuur 6-1, De feedbackuitvraag zoals deze in Xedule wordt aangeboden.

De persoonsgegevens die via deze uitvraag verzameld worden bestaan uit: taal, user ID (###@Institution.xedule.nl, waarbij ### de Xedule user ID is), responder code, institution en product (Xedule/MyXedule). Deze gegevens worden in Survicate ontsloten aan relatiemanagers, Product Owner pNPS en data-analisten van Xedule. Xedule kan instellingen benaderen ten behoeve van productverbetering op basis van deze informatie.

De user ID komt overeen met de ID in Xedule. Wanneer één van de personen die toegang heeft tot de gegevens in Survicate ook toegang heeft tot Xedule zijn de betrokkenen te herleiden. Hierdoor kunnen de geautoriseerden deze gegevens in de basis niet zomaar herleiden naar natuurlijke personen, maar de weg naar de-pseudonimisering is niet ver en ondenkbaar. Deze pseudonimisering is organisatorisch van aard.

Dezelfde dataset wordt ook doorgegeven aan het BigQuery platform van Google. Daar wordt het verwerkt in een dashboard wat samen met de data die voortvloeit uit andere processen (o.a. support) een beeld geeft over de klanttevredenheid op instellingsniveau.

De noodzaak van de verwerking van de user ID in latere stadia van de verwerkingen in Survicate en BigQuery, en daarmee de herleidbaarheid tot een natuurlijk persoon, is niet aangetoond.

Er is door Xedule geen duidelijkheid gegeven in de bewaartermijnen die gehanteerd worden binnen dit proces.

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 direct het anonimiseringsscript 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 niet 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).

Sinds najaar 2025 levert Xedule deze dienst niet meer onder de term anonimisering.

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.[22] 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.

Bronsysteem	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

[22] HPE Storage Security: https://www.hpe.com/psnow/doc/a00050848enw.

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:

7.7.2.1 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.

7.7.2.2 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.

7.7.2.3 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 via Connect ingesteld worden met behulp van standaard gedefinieerde categorieën: kalender, configuratie, onderwijs, faciliteiten, hrm, management informatie en student-informatie. Toegang tot de onderliggende dataset zijn gesegmenteerd in deze categorieën.

Xedule stelt dat een ander bijkomend voordeel is dat het beheer van API-keys door de instelling zelf gedaan kan worden, in plaats van handmatige aanvragen via de ontwikkelaars van Xedule.

7.7.2.4 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.

Bronsysteem	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 toezenden vanuit het bronsysteem naar het doelsysteem.

Bronsysteem	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

7.7.2.5 |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
Applicaction	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. De vijfde cookie betreft een sessie-identificatie (ASP.NET SessionId) die wordt gebruikt voor het authenticatieproces.

ai_session[23]
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_user[24]
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 persoonsgegeven.

---

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

[24] Microsoft Cookie Compliance - https://learn.microsoft.com/en-us/dynamics365/commerce/cookie-compliance

ARRAffinity en ARRAffinitySameSite[25]
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.

[25] 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.[26]

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.[27] De verwerker is de partij die persoonsgegevens alleen ten behoeve van de verwerkingsverantwoordelijke verwerkt.[28] 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). In de verwerkersovereenkomst vallen deze verwerkingen onder de doelen zoals beschreven in paragraaf 4.2 Verwerkingsdoeleinden instellingen verwerkersovereenkomst en zijn de precieze verwerkingen per doel uitgewerkt in de bijlage.

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

[26] 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.

[27] Artikel 4 sub 7 van de AVG.

[28] Artikel 4 sub 8 van de AVG.

medewerkers verwerkt worden, in welke mate en op welke manier. Dit maakt hen verantwoordelijk en dit geeft de verwerkersovereenkomst ook weer.

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 vanaf het moment van publicatie van deze DPIA, gebaseerd op de model Verwerkersovereenkomst versie 4.0, SURF Juridisch Normenkader (Cloud)services. De verwerkersdoelen die hierin zijn vastgelegd, zijn:

i) Beschikbaar stellen van de applicaties
ii) Bieden van ondersteuning aan de onderwijsinstelling
iii) Beveiliging van (persoons)gegevens die in de applicaties zijn opgenomen
iv) Technische verbeteringen van de applicatie zoals bugfixes, patchmanagement en onderhoud

De enige verwerkingen waarvoor Xedule van deze verwerkersrol mag afwijken zijn beschreven in paragraaf 8.3 Xedule: Gemachtigd verwerkingsverantwoordelijke.

8.3 Xedule: Gemachtigd verwerkingsverantwoordelijke

In overleg met Xedule zijn de verwerkingen in kaart gebracht die Xedule met gegevens die het als verwerker heeft verkregen uitvoert voor eigen doeleinden. Onder de verwerkersovereenkomst die Xedule sinds publicatie van deze DPIA aanbiedt verwerkt Xedule persoonsgegevens als gemachtigd verwerkingsverantwoordelijke voor de volgende vijf legitieme zakelijke doeleinden, uitsluitend voor deze vijf doeleinden en wanneer de verwerking strikt noodzakelijk en evenredig is:

1. Gebruiken van contactgegevens van medewerkers van de onderwijsinstelling die het functionele beheer van de applicaties verzorgen ten behoeve van:
    - Het efficiënt en effectief gebruiken van de applicaties
    - Serviceberichten zoals patchnotes, releasenotes en statusberichten
    - Bieden van ondersteuning bij vraagstukken
2. Gebruiken van contactgegevens van medewerkers van de onderwijsinstelling die betrokken zijn bij de dienstverlening ten behoeve van:
    - Contractuele verplichtingen zoals verlengingen, aanbestedingen, marktconsultaties, facturatie en inzet van medewerkers van Verwerker ter ondersteuning van de onderwijsinstelling
    - Verbeteringen en nieuwe functionaliteiten die buiten de dienstverlening vallen die in de bovenliggende overeenkomst opgenomen zijn
    - Onderwijslogistieke kennisoverdracht, innovatie en branchegerelateerde onderwerpen

3. Verzamelen van gegevens om te voldoen aan wettelijke verplichtingen, zoals het opvolgen van verzoeken tot verplichte verstrekking van persoonsgegevens vanuit autoriteiten en toepasselijke wetgeving met inachtneming van de overeengekomen voorwaarden in artikel 5 van de verwerkersovereenkomst.
4. Verzamelen van technische gegevens om noodzakelijke verandertrajecten in technische componenten van de applicaties te faciliteren.
5. *OPTIONEEL: keuze acceptatie bij verwerkingsverantwoordelijke* Verzamelen van gepseudonimiseerde scores en persoonsgegevens uit opmerkingenvelden bij functioneel beheerders, deze combineren met andere gegevens, ook van andere organisaties, deze aggregeren en contact opnemen met verwerkingsverantwoordelijke naar aanleiding van deze informatie teneinde de applicaties te verbeteren met inzichten van gebruikers.

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.[29] Een subverwerker is dus de verwerker van de verwerker.[30]

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. Bij wijziging van de subverwerkers kunnen instellingen bezwaar maken volgens de procedure vastgelegd in artikel 11.3 van de verwerkersovereenkomst.

Overzicht subverwerkers
In de Verwerkersovereenkomst is een overzicht opgenomen met subverwerkers waarvan Xedule gebruik maakt. Niet alle subverwerkers vallen onder de scope van deze DPIA. Die subverwerkers zijn grijs gemaakt.

[29] Artikel 28, lid 2 van de AVG.
[30] Verwerkingsverantwoordelijke of gegevensverwerker | European Data Protection Board

Subverwerker (naam incl. plaats van vestiging)	Persoonsgegevens die Subverwerker verwerkt	Omschrijving van de reden voor de subverwerking	Land van verwerking en relevant doorgifte instrument
Interconnect Datacenter Colocatie dienst. (Den Bosch) Wordt uitgefaseerd en vervangen door MS Azure	• Contactgegevens • Onderwijsorganisatie • Gebruiksgegevens • Overige Persoonsgegevens (niet zijnde bijzondere persoonsgegevens)	Hosting van platform op basis van colocatie waarbij datacenter medewerkers geen directe toegang hebben tot data.	Nederland
Contact Center Live (CCL) t.b.v. ondersteuning ticketsysteem (Uden)	• Contactgegevens • Onderwijsorganisatie • Gebruiksgegevens • Overige Persoonsgegevens (niet zijnde bijzondere persoonsgegevens)	Vanuit ondersteuning door CCL aan Xedule B.V. hebben de beheerders van CCL op aanvraag toegang tot het ticketsysteem van Xedule.	Nederland
Zendesk Inc. als ticketsysteem en informatiesysteem van Xedule B.V. (San Francisco)	• Contactgegevens • Onderwijsorganisatie • Gebruiksgegevens • Andere Persoonsgegevens (niet zijnde bijzondere persoonsgegevens)	Vanuit ondersteuning van medewerkers van de onderwijsinstelling worden tickets gemeld door onderwijsinstellingen waarin betreffende persoonsgegevens gebruikt worden. Zendesk wordt ingezet als informatietool voor onder meer patch- en releasenotes, functionele help en statusberichten	Duitsland

Synaxion B.V. (Eindhoven)	• Deelnemernummer • Personeelsnummer • Naam • E-mailadres	Dashboards, BI ten behoeve van rapportage behoeftes onderwijsinstellingen	Nederland
Microsoft Azure onder MS Norge AS contract (Oslo) Komt gefaseerd in de plaats van Interconnect	• Contactgegevens • Onderwijsorganisatie • Gebruiksgegevens • Andere Persoonsgegevens (niet zijnde bijzondere persoonsgegevens)	Schaalbare cloud infrastructuur t.b.v. hosten, opslaan en ontsluiten van My Xedule waarbij medewerkers van MS geen inhoudelijke toegang hebben tot data	Nederland
Innophase (Uden)	• Contactgegevens • Onderwijsorganisatie • Gebruiksgegevens • Andere Persoonsgegevens (niet zijnde bijzondere persoonsgegevens)	Medewerkers van onderwijsinstellingen kunnen deelnemen aan open opleidingen om getraind te worden in het gebruik van de applicatie(s)	Nederland
Escrow4All B.V. (Amsterdam)	• Contactgegevens • Onderwijsorganisatie • Gebruiksgegevens	Continuïteit Dienstverlening in opdracht van aanbestedende onderwijsinstellingen	Nederland

Tabel 8-1

De volgende subverwerkers zijn binnen scope van deze DPIA:

8.4.1 Interconnect

Interconnect is in Den Bosch gevestigd en volgens de hoofdovereenkomst met Interconnect neemt Advitrae Groep de colocatiedienstverlening van Interconnect af. Volgens Xedule is

het contract met deze rechtsvoorganger van Xedule overgegaan op Xedule.[31] Colocatie betekent dat Xedule haar eigen servers opslaat in de ruimtes van Interconnect. Interconnect levert daarbij rackspace, stroomvoorzieningen en internettoegang. In beginsel is een colocatiedienstverlener geen verwerker, als de dienstverlening niet bestaat uit het verwerken van persoonsgegevens. Relevant om te beoordelen of dit het geval is, zijn de volgende elementen:

- Of het bedrijf toegang heeft tot de persoonsgegevens, bijvoorbeeld toegang tot de serverkast, en kan toegang kan krijgen tot de gegevens die op de servers worden verwerkt;
- Of het bedrijf kan (en kan worden belast met) het vervangen van harde schijven, geheugen, enz. op de servers die zijn opgeslagen;
- Of het bedrijf de servers waar de gegevens worden verwerkt kan (en kan worden belast met het) verplaatsen, herstarten of anderszins behandelen;
- Of het bedrijf andere diensten biedt dan fysieke faciliteiten, stroom en internet.[32]

Het is uit de hoofdovereenkomst of algemene voorwaarden van Interconnect niet duidelijk of Interconnect toegang heeft tot de persoonsgegevens. Xedule heeft ook niet bevestigd dat de toegang tot de servers is afgesloten. Wel geven de algemene voorwaarden aan dat Interconnect in bepaalde gevallen de apparatuur mag uitschakelen en zich inspant om back-ups te maken, ook al maakt dit geen onderdeel uit van de opdracht van Xedule aan Interconnect. SURF heeft de documentatie die hier mogelijk verdere toelichting op biedt (Toelichting Colocatie Datacenter Eindhoven, Toelichting Colocatie datacenter 's Hertogenbosch en Addendum Twin Datacenter) niet ontvangen. Er moet op basis van de beschikbare documentatie dus aangenomen worden dat Interconnect gegevensverwerkingen kan uitvoeren en dus kwalificeert als verwerker. Xedule heeft echter geen subverwerkersovereenkomst met Interconnect.

8.4.2 Zendesk Inc. via Contact Center Live

Zendesk levert het platform dat Xedule gebruikt voor de online help en is gevestigd in de Verenigde Staten. Advitrae Groep, de voorganger van Xedule heeft een overeenkomst met Contact Center Live voor het gebruik van contact center producten en diensten. Advitrae groep (nu Xedule) is hierbij verwerkingsverantwoordelijke en CCL is verwerker. Xedule geeft aan dat de online help van Zendesk onder dit contract valt, maar hij is niet opgenomen als subverwerker. Daarnaast treedt Xedule op als verwerker bij het vertrekken van de online help, waardoor de kwalificatie van CCL subverwerker zou moeten zijn. Dit komt niet overeen met Xedules rol als verwerker voor de instellingen. De instellingen kunnen volgens deze contracten dus geen beroep doen op hun rechten als verwerkingsverantwoordelijke.

---

[31] E-mail van Xedule, 12 oktober 2026.

[32] Datatilsynet, *Skal leverandøren af colocation anses som databehandler? (vertaling: Moet de colocatieleverancier worden beschouwd als een gegevensverwerker?)*, https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/mar/skal-leverandoeren-af-colocation-anses-som-databehandler, geraadpleegd op 11 september 2026.

8.4.3 Synaxion B.V.

Synaxion is in Eindhoven gevestigd, valt ook onder de Visma Group en levert Business Intelligence (BI) diensten in de vorm van dashboards. Visma Advitrae, voorganger van Xedule, heeft een Intragroup Distribution Agreement met Synaxion. Volgens Xedule is het contract met deze rechtsvoorganger van Xedule overgegaan op Xedule.[33] Volgens de bepalingen van de overeenkomst treedt Visma Advitrae op als verwerker en Synaxion als subverwerker voor het gebruik van de Software van Synaxion. De 'end user', degene met wie Visma Advitrae als Distributor een licentieovereenkomst sluit is de verwerkingsverantwoordelijke. Als deze end user een instelling is, is de instelling dus verwerkingsverantwoordelijke voor de verwerkingen in de software van Synaxion, is Visma Advitrae verwerker en is Synaxion subverwerker.

Volgens Appendix 3 Data Processing Addendum, treedt Synaxion echter op als verwerker en Visma Advitrae als subverwerker. Dit is tegenstrijdig met de bepalingen van de overeenkomst, waarin dit andersom is.

8.4.4 Microsoft Norge AS

Xedule is de gegevens van de instellingen aan het migreren van de hosting op eigen servers (opgeslagen bij Interconnect) naar de Microsoft Azure cloud. Daarnaast maakt Xedule gebruikt van Azure insights. Visma AS heeft als moederbedrijf van Xedule een Microsoft Customer Agreement met Microsoft Norge AS voor het gebruik van Microsoft Azure Services. Het moederbedrijf van Microsoft Norge AS is in de Verenigde Staten gevestigd. De overeenkomst is van toepassing op 'orders' van licenties. Visma mag deze licentie-orders plaatsen voor gebruik door "Affiliates", waarbij de voorwaarden van de contracten van toepassing zijn op de Affiliate. Visma is de enige partij die de contractuele rechten bij Microsoft Norge AS kan afdwingen. Xedule heeft bevestigd dat het een Affiliate is waarvoor Visma licenties bestelt. Volgens de Data Protection Addendum treedt Microsoft op als subverwerker als de 'Customer' (Xedule in dit geval) optreedt als verwerker.

8.4.5 ESCROW4ALL

Advitrae Systems B.V. heeft een SaaS escrow mantelovereenkomst met ESCROW4ALL, gevestigd in Amsterdam, voor continuïteitsdiensten. Volgens Xedule is het contract met deze rechtsvoorganger van Xedule overgegaan op Xedule.[34] Volgens het Addendum Bijlage IV Sub-Verwerkersovereenkomst treedt ESCROW4ALL hierbij op als subverwerker voor Advitrae Systems als verwerker.

[33] E-mail van Xedule, 12 oktober 2026.

[34] E-mail van Xedule, 12 oktober 2026.

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 roosteringssysteem 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 overheidsinstanties zoals onderwijsinspectie en/of de arbeidsinspectie.

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

In de volgende paragrafen worden de doorgiftes beschreven die plaatsvinden als gevolg van het gebruik van de diensten van Xedule. Volgens het EDPB zijn de voorwaarden voor een overdracht:

1. „Een verwerkingsverantwoordelijke of een verwerker (‘exporteur’) valt voor de betreffende verwerking onder de AVG.
2. De exporteur stelt persoonsgegevens die onder deze verwerking vallen, door middel van verzending of op andere wijze ter beschikking aan een andere verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke of verwerker („importeur“).
3. De importeur bevindt zich in een derde land, ongeacht of deze importeur al dan niet onder de AVG valt voor de betreffende verwerking overeenkomstig artikel 3, of een internationale organisatie is.”[35]

10.1 Doorgiftes

Er vindt een aantal doorgiftes plaats naar partijen in derde landen bij het gebruik van Xedule en My Xedule, zoals opgenomen in de verwerkersovereenkomt.

10.1.1 Microsoft

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 deels gebruik van eigen servers, opgeslagen in 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.

Xedule is echter ook begonnen om de gegevens in Xedule en MyXedule van de servers in de datacenters van Interconnect te migreren naar hosting in de Azure cloud van Microsoft.[36] In de toekomst zullen alle gegevens gehost worden in de Microsoft Azure Cloud. Ook slaat Xedule een versleutelde back-up op bij Microsoft Azure. Xedule beheert hier zelf een encryptiesleutel voor. Xedule maakt daarnaast 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.

---

[35] EDPB, *Richtsnoeren 05/2021 over de wisselwerking tussen de toepassing van artikel 3 en de bepalingen inzake internationale doorgiften overeenkomstig hoofdstuk V van de AVG*, 14 februari 2023.

[36] Lijst van gebruikte Azurediensten: Application Insights; Key vault; Log Analytics workspace; Logic app; API connection; API connection; Private endpoint; Network Interface; Private endpoint; Network Interface; Storage account; SQL server; SQL database; SQL elastic pool; Private DNS zone; Private DNS zone; Virtual network; App Service.

Xedule maakt hierbij gebruik van de EU Data Boundary, wat betekent dat Microsoft in het algemeen 'Customer Data' opslaat op servers binnen EU-grenzen (regio West Europe).[37] Microsofts definitie van Customer Data is:

> *"Customer Data" means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, Customer through use of the Online Service. Customer Data does not include Professional Services Data."*[38]

Persoonsgegevens in door Microsoft gegenereerde logbestanden en persoonsgegevens in technische ondersteuningsdiensten ("Professionel Services data") van Microsoft vallen buiten deze definitie en dus buiten de EU Data Boundary.[39] Visma AS heeft een contract met Microsoft Norge AS, wat gevestigd is binnen de EER. Het verstrekken van gegevens aan Microsoft Norge is dus geen doorgifte. Microsoft Norge zou wel doorgiftes kunnen doen binnen de voorwaarden van de EU Data Boundary, aangezien er bepaalde uitzonderingen gelden op de EU Data Boundary voor alle Microsoftdiensten.[40] De relevante uitzonderingen voor Xedule zijn:

- Toegang tot Customer Data door personeel en opdrachtnemers van Microsoft voor ondersteuningsdoeleinden. Microsoft publiceert een overzicht van de landen van waaruit personeel toegang kan krijgen.[41]
- Het doorgeven van gepseudonimiseerde persoonsgegevens in zowel Professional Services data als Customer Data buiten de EU Data Boundary voor beveiligingsdoeleinden.

Daarnaast vallen Microsoft Content Delivery Network en Azure Front Door, die ervoor zorgen dat netwerkverkeer zo snel mogelijk bij de klant is via 'global edge locations' beiden buiten de EU Data Boundary.[42] Het is niet uit te sluiten dat de gegevens die hiervoor in cachegeheugen buiten de EU Data Boundary worden opgeslagen persoonsgegevens kunnen bevatten.

---

[37] Microsoft, *What is the EU Data Boundary?*, https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn, geraadpleegd op 14 september 2026.

[38] Microsoft Products and Services Data Protection Addendum, Last updated January 2, 2024.

[39] Microsoft, *What is the EU Data Boundary?*, https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn, geraadpleegd op 14 september 2026.

[40] Microsoft, *Continuing data transfers that apply to all EU Data Boundary Services*, https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services, geraadpleegd op 14 september 2026.

[41] Microsoft, *Locations of Microsoft Online Services Personnel with Remote Access to Data*, https://learn.microsoft.com/en-gb/microsoft-365/enterprise/personnel-loc/m365-personnel-location?view=o365-worldwide, geraadpleegd op 14 september 2026.

[42] Microsoft, *Services excluded from the EU Data Boundary*, https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-excluded-services, geraadpleegd op 14 september 2026.

Tot slot is het moederbedrijf van Microsoft AS gevestigd in de VS, waardoor Amerikaanse surveillancewetgeving en wetgeving inzake informatieverschaffing ook van toepassing is op verwerkingen van Microsoft AS.

SURF heeft de tests voor deze DPIA uitgevoerd op Xedule applicaties op Interconnect servers, en heeft dus niet technisch kunnen verifiëren of en welke verwerkingen en doorgiftes er plaatsvinden naar aanleiding van het gebruik van de Azure Cloud.

10.1.2 Zendesk

Xedule is recent gebruik gaan maken van Zendesk om hun online help aan te bieden, die onder anderen aanvullende informatie over de configuratie van de applicatieomgevingen bevat. Zendesk is gevestigd in de VS, dus verstrekking van persoonsgegevens aan Zendesk en toegang tot persoonsgegevens door Zendeskmedewerkers zijn doorgiftes. Xedule stelt dat Zendesk de online help host in Frankfurt. Volgens de verwerkersovereenkomst gebruikt Xedule Zendesk in het algemeen voor “Beheer, support en diagnostiek indien diensten onvoldoende vervuld kunnen worden door lokale beheerpartij binnen de EER”. Zendesk kan dus toegang krijgen tot persoonsgegevens via de online help ten behoeve van beheer, support en diagnostiek.

10.2 Doorgiftemechanismes

Momenteel is er een adequaatheidsbesluit van de Europese Commissie – het Data Privacy Framework – van toepassing op doorgiften tussen de EER en de VS. Microsoft en Zendesk zijn gecertificeerd onder het DPF, dus juridisch gezien geldt er een adequaat beschermingsniveau voor de doorgifte van persoonsgegevens aan Microsoft en Zendesk als. Recente ontwikkelingen hebben de pijlers van het DPF echter onder druk gezet, waardoor de bescherming in de praktijk niet meer overeenkomt met de juridische werkelijkheid.[43]

Mocht het DPF komen te vervallen, dan moet Xedule terugvallen op een alternatief doorgiftemechanisme. Modelcontractbepalingen (SCC’s) van de Europese Commissie maken deel uit van zowel het Microsoftcontract als het Zendeskcontract. Om hier een beroep op te kunnen doen, moet Xedule een Data Transfer Impact Assessment (DTIA) uitvoeren met betrekking tot hun doorgiftes.

[43] SURF, *(Sub)verwerkers in de Verenigde Staten*, https://vendorcompliance.surf.nl/subverwerkers-in-de-verenigde-staten/, geraadpleegd op 14 september 2026.

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 roosteringapplicatie 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

12.1.1 Xedule

In de verwerkersovereenkomst heeft Xedule de bewaartermijnen die bij de verschillende verwerkingen horen in de bijlage opgenomen. Voor de meeste gegevens binnen Xedule geldt dat de instelling de bewaartermijn bepaalt (zie paragraaf 12.1.2 Onderwijsinstelling). Voor de overige gegevens is de bewaartermijn in de verwerkersovereenkomst en de onderstaande tabel opgenomen.

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.

Categorie persoonsgegevens	**Bewaartermijn**
Applicatielogging in de productieomgeving	6 maanden
Applicatielogging in de acceptatieomgeving	3 maanden. (Logging wordt overschreven bij elke verversing van de acceptatieomgeving en is maximaal 3 maanden oud tenzij onderwijsinstellingen afzien van een verversing)
Internet Information Server (IIS) logging	6 maanden
Frond-End en Back-End logging	6 maanden
Windows servers logs	1 jaar
Firewall logs	6 maanden
Azure insights logs	90 dagen
Opt-out informatie pNPS	Direct na verwijderen gebruiker
Persoonsgegevens verzameld via pNPS	3 jaar

12.1.2 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 sinds het voorjaar van 2026 mogelijk om bewaartermijnen in te stellen op drie categorieën (datasets) binnen een ORE. Het is daardoor mogelijk om zelf te bepalen vanaf welk moment een bewaartermijn begint te lopen en de datasets worden overschreven met generieke data op het moment dat de de bewaartermijn is verstreken. Zie 5.1.6 Verwijdering van gegevens voor meer informatie.

Daarnaast kunnen functioneel beheerders van instellingen Xedule via een ticket instrueren persoonsgegevens te verwijderen.

12.2 Bewaartermijnen als verwerkingsverantwoordelijke

In de verwerkersovereenkomst zijn de verwerkingen opgenomen waarvoor Xedule als gemachtigd verwerkingsverantwoordelijke persoonsgegevens verwerkt. De bewaartermijnen hiervoor zijn als volgt.

Categorie persoonsgegevens	**Bewaartermijn**
Contactgegevens medewerkers functioneel beheer instelling	Zolang de onderwijsinstelling klant is en na beëindiging contract maximaal 6 maanden. Bij tussentijdse wisseling van medewerkers van de onderwijsinstelling direct verwijderd.
Contactgegevens commerciële medewerkers instelling	Zolang de onderwijsinstelling klant is en na beëindiging contract maximaal 6 maanden. Bij tussentijdse wisseling van medewerkers van de onderwijsinstelling direct verwijderd. Voorkeur voor algemene contactgegevens zoals een generieke mailbox.
Technische gegevens verandertrajecten	Maximaal 6 maanden na creatie log. Indien technische gegevens langer nodig zijn worden deze ontdaan van persoonsgegevens waarbij enkel de techniek bewaard blijft.
Klanttevredenheidsgegevens	3 jaar na verzameling

B. Beoordeling rechtmatigheid gegevensverwerkingen

13 Rechtsgrond

Een verwerkingsverantwoordelijke moet een grondslag hebben om persoonsgegevens rechtmatig te kunnen verwerken.[44] 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.[45] Om deze taak uit te kunnen voeren moeten instellingen planningen 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 een alternatieve mogelijkheid om ruimtes te reserveren bieden aan gebruikers die hun locatie niet willen delen 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 voeren. Ook hier moeten instellingen een noodzakelijkheidstoets uitvoeren om aan te tonen

[44] Art. 6 AVG.

[45] Zie art. 23 Grondwet, art. 1.3 WHW en art. 1.3 WEB.

dat het doel van de overeenkomst niet bereikt kan worden zonder de betreffende verwerkingen van persoonsgegevens.[46]

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.[47]

13.2 Grondslagen Xedule

Als verwerker is het Xedule niet toegestaan om gegevens die het heeft ontvangen als verwerker verder te verwerken voor andere doeleinden zonder toestemming van de instelling. Artikel 28 lid 10 van de AVG luidt:

> *"Indien een verwerker in strijd met deze verordening de doeleinden en middelen van een verwerking bepaalt, wordt die verwerker onverminderd de artikelen 82, 83 en 84 met betrekking tot die verwerking als de verwerkingsverantwoordelijke beschouwd."*

Xedule zou als verwerkingsverantwoordelijke in deze situatie geen geldige grondslag hebben. Om geldige verdere verwerkingen uit te voeren voor eigen doeleinden moeten de instellingen hier als verwerkingsverantwoordelijken toestemming voor hebben gegeven en moeten de verwerkingen volgens de toets van artikel 6 lid 4 AVG verenigbaar zijn met de originele doelen van de instellingen. Deze toets wordt gedaan 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.

---

[46] *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.

[47] Autoriteit Persoonsgegevens, *Grondslagen AVG uitgelegd*, https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/grondslagen-avg-uitgelegd#grondslag-gerechtvaardigd-belang, geraadpleegd op 2 mei 2025.

De nieuwe verwerkersovereenkomst bevat vijf doeleinden waarvoor Xedule als gemachtigd verwerkingsverantwoordelijke persoonsgegevens mag verwerken die het heeft ontvangen als verwerker, zoals beschreven in paragraaf 8.3 Xedule: Gemachtigd verwerkingsverantwoordelijke. Deze doelen zijn:

1. Gebruiken van contactgegevens van medewerkers van de onderwijsinstelling die het functionele beheer van de applicaties verzorgen ten behoeve van:
    - Het efficiënt en effectief gebruiken van de applicaties
    - Serviceberichten zoals patchnotes, releasenotes en statusberichten
    - Bieden van ondersteuning bij vraagstukken
2. Gebruiken van contactgegevens van medewerkers van de onderwijsinstelling die betrokken zijn bij de dienstverlening ten behoeve van:
    - Contractuele verplichtingen zoals verlengingen, aanbestedingen, marktconsultaties, facturatie en inzet van medewerkers van Verwerker ter ondersteuning van de onderwijsinstelling
    - Verbeteringen en nieuwe functionaliteiten die buiten de dienstverlening vallen die in de bovenliggende overeenkomst opgenomen zijn
    - Onderwijslogistieke kennisoverdracht, innovatie en branchegerelateerde onderwerpen
3. Verzamelen van gegevens om te voldoen aan wettelijke verplichtingen, zoals het opvolgen van verzoeken tot verplichte verstrekking van persoonsgegevens vanuit autoriteiten en toepasselijke wetgeving met inachtneming van de overeengekomen voorwaarden in artikel 5.
4. Verzamelen van technische gegevens om noodzakelijke verandertrajecten in technische componenten van de applicaties te faciliteren.
5. *OPTIONEEL: keuze acceptatie bij verwerkingsverantwoordelijke* Verzamelen van gepseudonimiseerde scores en persoonsgegevens uit opmerkingenvelden bij functioneel beheerders, deze combineren met andere gegevens, ook van andere organisaties, deze aggregeren en contact opnemen met verwerkingsverantwoordelijke naar aanleiding van deze informatie teneinde de applicaties te verbeteren met inzichten van gebruikers.

Verband tussen de doeleinden (a)
Het gebruiken van contactgegevens voor serviceberichten en commerciële communicatie en het faciliteren van een soepele overgang naar nieuwe technische componenten van de applicatie hebben een duidelijk verband met het doel van de instellingen om een goed werkende en veilige applicatie te hebben. Verder hebben instellingen geen andere keuze dat het accepteren van het feit dat Xedule moet voldoen aan zijn wettelijke verplichtingen om gegevens te verstrekken onder bepaalde voorwaarden.

Kader verzameling gegevens (b)

De gegevens zijn verzameld bij de instellingen en in de applicatie en de manier waarop dat gebeurt is vastgelegd in de verwerkersovereenkomst. De verwerkingen zijn allemaal in lijn met de redelijke verwachtingen die een gebruiker van de applicaties kan hebben, omdat ze niet verder gaan dan wat nodig is voor een goed functionerende applicatie en de wettelijke verplichtingen die een leverancier heeft. Ten gevolge van deze beoordeling hebben instellingen ingestemd met de verdere verwerkingen en ervoor gezorgd dat deze alleen binnen de kaders van de verwerkersovereenkomst kunnen plaatsvinden. Hiermee vervullen de instellingen en Xedule samen hun verantwoordelijkheid naar de betrokkenen.

Aard van de persoonsgegevens (c)
De relevante persoonsgegevens zijn contactgegevens en technische gegevens, zoals besturingssystemen en browserversies. De gegevens worden waar mogelijk gepseudonimiseerd en er is verder geen indicatie dat ze bijzondere of gevoelige gegevens bevatten.

Gevolgen voor betrokkenen (d)
De gevolgen voor betrokkenen zijn dat ze ongewenst benaderd kunnen worden en dat hun gegevens (eventueel zonder hun medeweten) gedeeld kunnen worden. Zo kunnen ze de controle verliezen over wat er met hun gegevens gebeurt.

Passende waarborgen (e)
Om de impact en waarschijnlijkheid van deze gevolgen te beperken is er in de verwerkersovereenkomst precies vastgelegd met welke doeleinden van Xedule de instellingen hebben ingestemd. Xedule mag deze doeleinden dus niet zelfstandig uitbreiden. Ook worden de gegevens waar mogelijk gepseudonimiseerd. Daarnaast is in de verwerkersovereenkomst vastgelegd dat Xedule alleen onder strikte voorwaarden haar geheimhoudingsplicht met betrekking tot de persoonsgegevens mag breken. Xedule treedt (indien toegestaan) eerst in overleg als het een verzoek tot verstrekking ontvangt en handelt alleen als dit moet volgens toepasselijke wetgeving of een rechterlijke uitspraak.

Onder deze omstandigheden zijn de verwerkingen van Xedule zoals vastgelegd in de verwerkersovereenkomst dus verenigbaar met de originele doelen van de instellingen. Xedule moet zelf kunnen aantonen dat het een grondslag heeft voor deze verwerkingen. Daar is in het kader van deze DPIA geen onderzoek naar gedaan.

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.[48] 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

[48] Autoriteit Persoonsgegevens, *Regels voor werkgevers bij zieke werknemers,* https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/zieke-werknemers/regels-voor-werkgevers-bij-zieke-werknemers, 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. Xedule biedt instellingen de mogelijkheid om de redenen voor afwezigheid te definiëren en te labelen welke redenen met ziekte te maken hebben, zodat instellingen hun systeem binnen wettelijke kaders in kunnen richten.

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 Grondslagen Xedule is al uitgewerkt dat de verdere verwerkingen die Xedule uitvoert met de persoonsgegevens die het bedrijf via de instellingen heeft verkregen verenigbaar zijn met de originele doelen.

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 dat een overkoepelend overzicht bemoeilijkt 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.

De betrokkenen mogen en kunnen redelijkerwijs verwachten dat hun persoonsgegevens worden gebruikt voor roostering en planning, en voor de doeleinden zoals beschreven in paragraaf 13.2 Grondslagen Xedule. 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. Deze DPIA heeft de volgende waarborgen geïdentificeerd die noodzakelijk zijn om te zorgen dat de inbreuk op de privacy van betrokkenen niet verder gaat dan noodzakelijk voor het doel:

- Xedules verdere verwerkingen voor eigen doeleinden beperken tot het noodzakelijke
  In de nieuwe verwerkersovereenkomst met Xedule is een uitputtende lijst opgenomen van de doeleinden waarvoor Xedule als gemachtigd verwerkingsverantwoordelijke gegevens mag verwerken. Er is ook vastgelegd dat de verwerkingen voor deze doeleinden tot het noodzakelijke en proportionele beperkt worden en dat Xedule de lijst niet zelfstandig kan uitbreiden.
- Betrokkenen er in de context van de applicatie voor waarschuwen dat ze geen gevoelige of bijzondere persoonsgegevens in de vrije velden moeten invullen.
  Xedule informeert gebruikers via een informatie-icoon bij open velden met de volgende tekst: “Voer geen bijzondere en gevoelige persoonsgegevens in, tenzij dit volgens je instellingsbeleid mag.” Zo blijft de aanwezigheid van dit type gegevens beperkt tot het minimum en binnen de kaders die de instellingen hebben vastgesteld.
- Het verwijderen van identificerende gegevens van de beoordelingen die betrokkenen in reactie op de feedbackuitvraag geven.
  Xedule verwijdert de user ID en de responder code van de ontvangen beoordelingen na ontvangst in Survicate en voor het doorsturen naar BigQuery. Op deze manier

worden de reacties gepseudonimiseerd – en geanonimiseerd als ook het tekstveld wordt verwijderd – waardoor de inbreuk op de privacy van de betrokkenen tot een minimum beperkt wordt.

- Technisch verhinderen – of op zijn minst bemoeilijken – dat gebruikers gegevens uit de interfacetabellen kunnen kopiëren buiten de applicatie.
  Xedule zorgt er in de app-based versie van de applicatie voor dat gegevens niet uit de interfacetabellen naar buiten de applicatie kunnen worden gekopieerd, tenzij instellingen dit toestaan. Dit is in de web-based versie van de applicatie niet mogelijk, dus Xedule geeft een pop-up wanneer gebruikers CTRL+C gebruiken met een waarschuwing om gegevens niet buiten de applicatie te kopiëren, tenzij dit volgens hun instellingsbeleid is toegestaan. Dit zorgt ervoor dat er niet meer kopieën van dezelfde persoonsgegevens worden gecreëerd dan noodzakelijk.
- De mogelijkheid bieden om een centraal RBAC-systeem te koppelen.
  Voor instellingen die gebruik willen maken van een centraal RBAC-systaan om hun autorisaties te beheren, biedt Xedule deze mogelijkheid. Zo hoeven er geen dubbele verwerkingen verricht te worden om dezelfde autorisaties te verlenen.
- Instellingen de actieve keuze bieden om de feedbackuitvraag aan of uit te zetten.
  Xedule informeert nieuwe klanten bij implementatie dat ze een keuze moeten maken of ze feedbackuitvraag in de applicatie aan of uit willen zetten. Er is geen standaardconfiguratie. Instellingen moeten dus deze keuze manier, afhankelijk van of deze functionaliteit noodzakelijk is voor hun bedrijfsprocessen.
- De mogelijkheid om automatische bewaartermijnen in te kunnen stellen.
  Handmatige processen voor gegevensverwijdering zijn foutgevoelig. Xedule biedt in plaats daarvan de mogelijkheid om per ORE automatische bewaartermijnen in te stellen, zodat gegevens niet langer worden bewaard dan noodzakelijk.
- Zorgen dat de persoonlijke redenen voor afwezigheid niet via een open tekstveld automatisch worden gedeeld met de roosteraar.
  Xedule heeft de inrichting van My Xedule aangepast, zodat gebruikers geïnformeerd worden of het open tekstveld dat ze kunnen invullen bij het doorgeven van hun afwezigheid gedeeld wordt met de roosteraar. Ook kunnen instellingen er binnenkort voor kiezen dat deze tekstvelden nooit worden gedeeld met de roosteraar, aangezien deze niet in alle gevallen de informatie uit dit veld nodig heeft.
- De API's laten differentiëren tussen de gegevens die er met de API-sleutel opgehaald kunnen worden.
  De REST API en SOAP API geven ongedifferentieerd toegang tot de gegevens in de applicaties. Om te voorkomen dat deze toegang onnodig breed wordt gegeven, kunnen instellingen via Connect de toegang per sleutel beperken tot het noodzakelijke.

Sinds Xedule de noodzakelijke, beschreven maatregelen heeft genomen, is het voor instellingen mogelijk om de applicaties op een proportionele manier in te zetten.[49]

[49] Een aanvullende waarborg waar Xedule meer bij zou kunnen ondersteunen, is om geen velden voor persoonsgegevens aan te bieden die niet noodzakelijk zijn voor de hoofddoelen waarvoor Xedule en My Xedule worden aangeboden. Instellingen kunnen 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.

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.

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 (verwerkingsverantwoordelijke)**	**Xedule (verwerker)**
Recht op inzage	Instellingen kunnen volledige inzage geven in accountdata en contentdata.	Xedule verstrekt de aanvullende systeemlogging die niet beschikbaar is in de applicatie.
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.	Xedule verwijdert gegevens op verzoek van de instelling of als de door de instellingen geautomatiseerde bewaartermijnen verlopen.
Recht op beperking	Accountdata en contentdata kunnen worden beperkt wanneer hier overeenstemming over is tussen onderwijsinstelling en betrokkene.	Xedule beperkt verwerkingen op verzoek van de instelling.
Recht van bezwaar	Betrokkenen kunnen hun recht op bezwaar inroepen bij de instelling. De instelling kan zelf	Xedule stopt verwerkingen op verzoek van de instelling.

	de benodigde handelingen met de contentdata en accountdata uitvoeren.	

Voor de verwerkingen waar Xedule zelf verantwoordelijk voor is, is Xedule ook verantwoordelijk voor het beantwoorden van inzageverzoeken. SURF heeft voor de verdere verwerkingen geïdentificeerd in de verwerkersovereenkomst (zie paragraaf 8.3 Xedule: Gemachtigd verwerkingsverantwoordelijke en 13.2 Grondslagen Xedule) geen afzonderlijk inzageverzoek gedaan. Xedule heeft in het inzageverzoek als verwerker wel aangetoond dat het inzage kan verschaffen in alle persoonsgegevens beschreven in deze DPIA, waaronder degene die het als gemachtigd verwerkingsverantwoordelijke verwerkt.

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.[50] Hierbij wordt een objectieve inschatting gemaakt van de kans (waarschijnlijkheid) en impact (ernst) van mogelijke negatieve gevolgen, zoals fysieke, emotionele of materiële schade.[51] 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.

[50] How do we do a DPIA?, 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.
[51] Overview of Data Protection Harms and the ICO's Taxonomy, 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			

Deze versie van de DPIA is een update op de eerste versie die op 8 juli 2025 is gepubliceerd. De onderstaande tekst is de ongewijzigde tekst zoals die op 8 juli 2025 is gepubliceerd met de risico's die destijds zijn geïdentificeerd. In de tekstblokken staan de updates op deze risico's, met de maatregelen die Xedule sinds de eerste versie van de DPIA heeft getroffen en de nieuwe risicoinschatting. Daarnaast is er een nieuwe risico ontstaan na publicatie van de eerste versie, die als risico 18.19 een in los tekstvak onderaan dit hoofdstuk is opgenomen.

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 systeemloggingggegevens (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.

Xedule heeft de verwerkersovereenkomst vernieuwd. In de nieuwe versie is er een duidelijk onderscheid tussen de doelen waarvoor Xedule verwerkingen doet als verwerker en als gemachtigd verwerkingsverantwoordelijke. Zie voor een overzicht van deze doelen: 8.2 Xedule: Verwerker en 8.3 Xedule: Gemachtigd verwerkingsverantwoordelijke. Met de persoonsgegevens die Xedule verkrijgt als verwerker mag het een beperkt aantal verwerkingen uitvoeren voor eigen doeleinden, waar instellingen in de verwerkersovereenkomst mee akkoord gaan. Xedule voert geen verwerkingen uit als zelfstandig verwerkingsverantwoordelijke (zoals vastgelegd in de privacyverklaring) met gegevens die het verkregen heeft als verwerker.

Hiermee kan het risico zich niet meer voordoen, waardoor de kans naar laag is gebracht. Het resterende risico is dus laag.

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 pseudonimisering 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.

Xedule heeft een loggingbeleid opgesteld. Dit beleid kan bij Xedule worden opgevraagd en is uiterlijk 31 maart 2027 beschikbaar via een webpagina. Het loggingbeleid bevat een overzicht van de gegevens die worden vastgelegd, de doelen van de logging per gegeven en de bewaartermijnen. Het loggingbeleid is echter vrij summier en sluit niet aan op de resultaten van het inzageverzoek met betrekking tot Azure Insights monitoring. Volgens het beleid vindt dit wel plaats, maar in het onderschepte dataverkeer van de tests voor deze update op de DPIA is dit niet gedetecteerd. Aan de hand van het loggingbeleid is ook niet vast te stellen welke gebeurtenissen er in het kader van deze monitoring plaats hadden moeten vinden.
Ook wordt er in het beleid niet beschreven op welke manier Xedule aan read access logging doet.

Het inzageverzoek was uiteindelijk wel compleet, nadat Xedule ook de firewall logs en read access logs heeft geleverd.

Xedule heeft ook aanvullend inzicht verschaft in hun pNPS-verwerkingen. Deze zijn nu ook opgenomen in de verwerkersovereenkomst onder de verwerkersdoelen.

Aangezien er een discrepantie is tussen het loggingbeleid en de feitelijke loggingpraktijken, en aan de hand van het loggingbeleid niet kan worden bepaald waar dit door komt, is de kans dat dit risico zich voordoet nog steeds hoog. Het risico blijft hiermee hoog.

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.

Xedule heeft de interface voor het beheren van wijzigingsredenen aangepast. Dit beheer gebeurt door middel van een label dat laat zien waarom iemand afwezig is, waardoor het rooster moet worden gewijzigd. In de nieuwe interface worden instellingen bij het configureren van de wijzigingsredenen (labels) gedwongen om bewust te bepalen wie de wijzigingsreden kan inzien (bijvoorbeeld roosteraard of leidinggevenden) en of de wijzigingsreden een gezondheidsgegeven is (afwezigheid door ziekte). De manier waarop de interface is ingericht confronteert gebruikers met de configuratiekeuzes die ze maken.

De nieuwe inrichting van de interface heeft – in combinatie met de maatregelen die instellingen zelf moeten treffen om te voorkomen dat ze onnodig brede afwezigheids- en hulpmiddelencategorieën definiëren – een voldoende waarschuwende functie om de kans dat dit risico zich voordoet naar laag te brengen. Hiermee is het risico laag geworden.

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.

Xedule heeft het overzicht van de subverwerkers in de verwerkersovereenkomst naar de actuele situatie aangepast. Er is dus een volledig overzicht van de leveranciers die optreden als subverwerkers.

Ook heeft Xedule heeft inzage gegeven in de hoofdovereenkomsten en subverwerkersovereenkomsten met deze leveranciers. Deze overeenkomsten laten echter zien dat Xedule niet bij alle leveranciers contractueel gezien de verwerkersrol heeft, en de leverancier de subverwerkersrol. Ook zijn de aangeleverde contracten niet allemaal tussen Xedule en de leverancier, maar in sommige gevallen tussen Visma en de leverancier.

- Met Interconnect ontbreekt de subverwerkersovereenkomst. Bij deze partij is het nog mogelijk dat deze niet optreedt als subverwerker, maar dit heeft Xedule niet kunnen aantonen.
- Volgens het contract met Zendesk is Xedule verwerkingsverantwoordelijke.
- De appendix bij het contract met Synaxion stelt dat Xedule subverwerker is, in plaats van verwerker.

De contractuele rolverdeling tussen Xedule en subverwerkers is in deze gevallen dus onduidelijk of anders dan feitelijk is vastgesteld in deze DPIA. Instellingen kunnen contractueel gezien dus niet in alle gevallen een beroep doen op hun rol als verwerkingsverantwoordelijke en zo hun controle over de verwerking van de persoonsgegevens via deze leveranciers uitoefenen, bijvoorbeeld bij inzageverzoeken en datalekken.

De kans dat er een verlies van controle optreedt is waarschijnlijk, aangezien er contractuele waarborgen missen. De impact hiervan is zwaar, omdat het hier grote groepen persoonsgegevens bij verschillende subverwerkers (leveranciers) betreft. Daarmee is dit een hoog risico.

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 leidinggevenden van deze beschikbaarheidsopgaven worden deze inclusief persoonlijke motivaties automatisch doorgestuurd naar roosteraars. Leidinggevenden 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.

Xedule biedt instellingen na wijzigingen in de applicatie nu de mogelijkheid om het motivatieveld uit te schakelen. Hiermee kan de gebruiker helemaal geen motivatie meer toevoegen. Als de functie actief blijft, waarschuwt het systeem de gebruiker tekstueel dat zowel de leidinggevende als de roosteraar de motivatie kunnen inzien.

Voor instellingen die geen noodzaak hebben voor het toevoegen van motivaties brengt de eerste optie de waarschijnlijk dat dit risico zich voordoet naar laag. Voor instellingen die deze informatie wel nodig hebben voor hun bedrijfsprocessen brengt de nieuwe waarschuwing de kans dat er vertrouwelijke informatie onnodig verstrekt wordt omlaag naar redelijk, in plaats van waarschijnlijk. Gebruikers krijgen hierdoor namelijk de kans hun motivatie te herformuleren als ze niet willen dat de roosteraar inzicht krijgt in gevoelige, persoonlijke informatie. Hiermee is het risico naar medium gedaald.

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.

Xedule heeft een informatieknop bij het veld geplaatst, zodat een roosteraar een waarschuwing ziet. Deze waarschuwing luidt als volgt: “Dit is een vrij tekstveld. Vul hier uitsluitend noodzakelijke en functionele informatie in conform het beleid van je onderwijsinstelling.” Deze tekst wordt nog aangepast naar: “Voer geen bijzondere en gevoelige persoonsgegevens in, tenzij dit volgens je instellingsbeleid mag.” Het icoon verduidelijkt dat aandacht nodig is, terwijl de interactie inzicht geeft in het gebruik en het doel van het vrije veld. Omdat gebruikers door deze maatregel worden gewaarschuwd om alleen gegevens binnen het beleid van hun instelling in te voeren, is de kans dat er een verlies van controle over (gevoelige) gegevens optreedt laag, mits de instellingen de maatregelen aan hun kant ook uitvoeren.

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 onterecht 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.

Bij dit risico waren er geen maatregelen voor Xedule vastgesteld.

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.

Xedule heeft nieuwe functies toegevoegd aan de inrichting van een Onderwijs Rooster Eenheid (ORE). Hierdoor kan de instelling bewaartermijnen koppelen aan drie datasets die gekoppeld zijn aan een ORE: medewerkerdata, studentendata en opmerkingen. Na het verstrijken van deze termijn worden deze datasets automatisch overschreven met generieke data die geen persoonsgegevens bevatten. Het blijft onduidelijk of bijzondere persoonsgegevens, zoals wijzigingsredenen en verlofgegevens, hiermee ook verwijderd worden, of dat die ook op centrale plekken opgeslagen zijn die niet gekoppeld zijn aan een ORE. Xedule geeft aan dat deze functionaliteit nog in ontwikkeling is, in overleg met verwerkingsverantwoordelijken.

Deze maatregelen verlagen de kans dat een instelling de controle over bewaartermijnen verliest. Aangezien het niet duidelijk is of alle gegevens – waaronder gevoelige (verlof- en verzuim)gegevens – onder deze maatregel vallen, blijft de kans wel redelijk, in plaats van waarschijnlijk. Daarmee blijft het risico hoog.

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.

Xedule heeft binnen de gestelde termijn van dertig dagen gegevens verstrekt naar aanleiding van het nieuwe inzageverzoek dat SURF heeft gedaan voor deze update. Deze dataset was onvolledig. De volgende gegevens ontbraken:

- Azure Insights logs;
- Firewall logs;
- Welke data is ingezien door de gebruiker in de Read Access logs.

Daarnaast heeft Xedule de logs verstrekt in losse lijsten van logs, zonder context of uitleg, bijvoorbeeld in een readme bestand. Er was ook geen koppeling met het loggingbeleid, zodat duidelijk was welke log entry bij welk onderdeel van het beleid hoorde.

De reactie op het inzageverzoek bevatte meer informatie dan bij het vorige inzageverzoek, maar was niet compleet. Daarnaast is de informatie niet in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm verstrekt. De kans dat het recht op inzage niet kan worden uitgevoerd is dus redelijk, waardoor het risico hoog blijft.

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.

Xedule heeft het gebruik van door Xedule verstrekte import templates voor csv-bestanden verplicht gesteld.

Hiermee is de kans dat er verlies van controle optreedt laag geworden, en het risico ook.

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.

Xedule is voornemens om technische maatregelen te treffen zodat in de xxx versie gebruikers gewaarschuwd worden bij het kopiëren van data en bij de xxx versie gekopieerde data alleen binnen Xedule te plakken is. Deze maatregelen zijn nog niet uitgevoerd.

Aangezien er niets is veranderd, blijft het risico onverminderd hoog. Instellingen kunnen de kans dat er een verlies van controle optreedt wel zelf verminderen door de maatregelen zoals beschreven in deel D te treffen, maar niet voldoende om het risico te mitigeren naar laag.

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.

Xedule heeft aangegeven hier geen ontwikkeling in te hebben gestart, maar bevestigt dat het ervoor zal zorgen dat instellingen die Xedule willen koppelen aan een centrale RBAC dit kunnen doen. Indien instellingen gebruik maken van deze optie om hun rollen actueel te houden, wordt de kans dat er verlies van vertrouwelijkheid optreedt naar laag gebracht en is het risico dus laag.

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 autorisatiewijzingen 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.

Xedule heeft geen wijzigingen in de interface aangebracht. Het risico is onverminderd hoog.

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.

Xedule heeft het Xedule Connect platform beschikbaar gesteld, waardoor instellingen zelf API-koppelingen kunnen beheren. Elke koppeling krijgt hiermee eigen sleutels. De standaard Xedule REST-koppeling is uitgebreid: instellingen kunnen per koppeling een sleutel aanvragen voor lezen of schrijven. Het Xedule Connect platform is nu een aanvullende dienst die afzonderlijk moet worden afgenomen. Als instellingen gebruik maken van dit platform, is de kans op verlies van vertrouwelijkheid door de configuratie van de REST API laag. Het risico is daarmee ook laag.

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.

Xedule heeft instellingen benaderd om over van de SOAP API over te stappen naar de REST API. Als de instellingen gebruik maken van deze mogelijkheid, is de kans dat er verlies van vertrouwelijkheid optreedt laag. Het risico is daarmee ook laag.

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 verlofgegevens 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.

Xedule heeft alle verwijzingen naar anonimisering in verwijzing naar deze verwerking verwijderd. Dit vermindert de kans dat instellingen de datasets als anoniem beschouwen naar laag, waardoor het risico laag is.

18.17 Heridentificering gepseudonimiseerde pNPS-gegevens

De gegevens die verwerkt worden om klantfeedback via pNPS te analyseren, worden volgens Xedule[52] gepseudonimiseerd voordat deze in een big data-applicatie worden opgeslagen. Analisten van Xedule hebben toegang tot deze gepseudonimiseerde gegevens. Volgens Xedule[53] 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.

[52] Mailwisseling met CISO van Xedule.

[53] Mailwisseling met CISO van Xedule.

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.

Xedule biedt nieuwe klanten nu actief de keuze om pNPS aan of uit te zetten. Er is geen standaardkeuze. Eerder heeft Xedule al een inventarisatie gedaan van welke klanten gebruik willen maken van de functionaliteit, en hen nogmaals geïnformeerd over de mogelijkheid de functionaliteit uit te zetten via nieuwsbrief.

Xedule heeft Wootric uitgefaseerd en gebruikt nu Survicate om pNPS-feedback te verzamelen. De input van roosteraars en admins wordt gepseudonimiseerd verwerkt, waarbij de user-id overeenkomt met die in Xedule. De dataset wordt ook doorgegeven aan Bigquery voor dashboards over klanttevredenheid. De noodzaak van herleidbaarheid in zowel Survicate als BigQuery is niet aangetoond en Xedule heeft niet aangetoond dat de user-ID en andere identificerende gegevens op enig moment worden verwijderd of vervangen. Er is wel een bewaartermijn van twee jaar in de verwerkersovereenkomst opgenomen voor deze gegevens, maar Xedule kon niet vaststellen of deze in de praktijk wordt nageleefd.

De kans dat er heridentificering optreedt is dus nog steeds hoog, omdat het niet duidelijk is wanneer de onnodig identificerende gegevens worden verwijderd. Het risico blijft hiermee hoog.

18.18 Verlies van vertrouwelijkheid door 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.

De Read Access-logs die Xedule als reactie op de inzageverzoeken heeft geleverd, waren op cruciale punten onvolledig. Xedule heeft aangegeven de logs alsnog te kunnen genereren, maar ondervindt moeilijkheden bij aanleveren van de logs in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm.

Aangezien SURF nog geen inzage heeft gekregen in de read access logs, blijft de kans dat er verlies van vertrouwelijkheid optreedt hoog en blijft het risico dus ook hoog.

18.19 NIEUW Verlies van controle door verplichte openbaarmaking of onbevoegde toegang in derde landen

Door het gebruik van Microsoftdiensten, zoals beschreven in 10.1.1 worden er ondanks het gebruik van de EU Data Boundary persoonsgegevens doorgegeven aan derde landen. In de verwerkersovereenkomst is ook opgenomen dat er doorgiftes plaatsvinden naar Zendesk, maar het is onduidelijk welke dit zijn. Daarnaast is VS surveillancewetgeving en openbaarmakingswetgeving van toepassing op Zendesk als Amerikaans bedrijf en op Microsoft AS als bedrijf met een Amerikaans moederbedrijf.

De impact van een verlies van controle door doorgifte kan zwaar zijn. Hoewel het Data Privacy Framework onder druk staat, is de kans op schade voor betrokkenen laag zo lang het nog bestaat. Dit risico is dus laag. Mocht het DPF vervallen, dan moeten instellingen een alternatief doorgiftemechanisme gebruiken en moet Xedule mogelijk een DTIA doen.

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 tijdlijn voor de acties.

De vastgestelde risico's en noodzakelijke maatregelen om die te mitigeren zijn niet veranderd ten opzichte van de eerste versie van de DPIA, dus onderstaande tabellen zijn onveranderd. Ze laten alleen zien welke maatregelen nodig zijn om de risico's te mitigeren, niet de actuele status van de risico's. Die is te vinden in de statustabel in de samenvatting. Wel is er een nieuw risico met maatregelen toegevoegd aan dit hoofdstuk.

Verlies van controle door Xedule als verwerkingsverantwoordelijke						
Referentie	**Aanleiding**	**Gevolg**	**Kans**	**Impact**	**Risicoscore**	
	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**	
18.1	-	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	Restrisico

Tabel 19-1, Verlies van controle door Xedule als verwerkingsverantwoordelijke

Voorgestelde actie(s) Xedule	Tijdlijn
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**	
	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**	
18.2		Inzage verschaffen in alle verwerkingen bij inzageverzoeken	Minimaal	Zwaar	Laag	Restrisico
		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				

Tabel 19-2, Verlies van controle door gebrek aan transparantie logging, pNPS en marketing

Mitigerende actie Xedule	Tijdlijn
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
	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	
	Maatregelen Instelling	**Maatregelen Leverancier**	**Kans**	**Impact**	**Risico-score**	
18.3	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	Restrisico
	Duidelijke training en instructie over welke gegevens wel en niet in open velden mogen worden geregistreerd					
	Monitoring van de effectiviteit van dit beleid					

Tabel 19-3, Verlies van vertrouwelijkheid en sociaal nadeel door te brede definiëring afwezigheids- en hulpmiddelencategorieën

Mitigerende actie Xedule	**Tijdlijn**
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
	Gebrek aan transparantie subverwerkers	Niet mogelijk om AVG-rechten volledig uit te oefenen voor betrokkenen en verlies van controle instellingen	Waarschijnlijk	Zwaar	Hoog	
	Maatregelen Instelling	**Maatregelen Leverancier**	**Kans**	**Impact**	**Risico-score**	
18.4	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	Restrisico

Tabel 19-4, Niet mogelijk om AVG-rechten uit te oefenen en verlies van controle door gebrek aan transparantie subverwerkers

Mitigerende actie Xedule	**Tijdlijn**
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	
	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				

Tabel 19-5, Verlies van vertrouwelijkheid door doorgeven beschikbaarheidsredenen aan roosteraars

Mitigerende actie Xedule	**Tijdlijn**
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	
	Maatregelen Instelling	**Maatregelen Leverancier**	**Kans**	**Impact**	**Risicoscore**	
	Duidelijke training en instructie over welke gegevens wel en niet in open velden mogen worden geregistreerd Monitoring van de effectiviteit van dit beleid	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	Restrisico

Tabel 19-6, Verlies van controle en vertrouwelijkheid door overige vrije velden

Mitigerende actie Xedule	Tijdlijn
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

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	
	Maatregelen Instelling	**Maatregelen Leverancier**	**Kans**	**Impact**	**Risicoscore**	
	Training roosteraars Automatiseren invoer waar mogelijk	-	Laag	Enige	Laag	Restrisico

Tabel 19-7, Gemiste kansen en verlies van vertrouwelijkheid door handmatige invoer

Mitigerende actie Xedule	Tijdlijn
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
	Geen automatische bewaartermijnen	Verlies van controle en vertrouwelijkheid	Hoog	Hoog	Hoog	
	Maatregelen Instelling	**Maatregelen Leverancier**	**Kans**	**Impact**	**Risicoscore**	
18.8	Vaststellen en beheren bewaartermijnen persoonsgegevens	Technische configuratie en beheer van bewaartermijnen per groep persoonsgegevens faciliteren	Laag	Hoog	Laag	Restrisico
	Naleving bewaartermijnen vastleggen in processen	Inzichtelijk maken procedure verwijderen persoonsgegevens door middel van een verzoek aan Xedule				
	NIEUW Xedule voorzien van de benodigde informatie om verdere functionaliteiten te ontwikkelen voor het automatisch configureren van bewaartermijnen.					

Tabel 19-8, Verlies van controle en vertrouwelijkheid door niet automatisch te configureren bewaartermijnen

Mitigerende actie Xedule	Tijdlijn
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
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.	

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	
	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	Restrisico

Tabel 19-9, Niet uit kunnen oefenen van AVG-rechten door incomplete inzageverzoeken

Mitigerende actie Xedule	**Tijdlijn**
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
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)	

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	
	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	Restrisico

	Duidelijke training en instructie voor degenen die gebruik moeten maken van handmatige import/export	Automatische import/export faciliteren waar mogelijk				

Tabel 19-10,Verlies van controle en vertrouwelijkheid door het niet hebben van automatische import/export

Mitigerende actie Xedule	Tijdlijn
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
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.	

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	
	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	

Tabel 19-11, Verlies van controle en vertrouwelijkheid door tabellen

Mitigerende actie Xedule	Tijdlijn
Onderzoek welke tabellen relevant zijn om te blokkeren of configurabel te maken om data te kopieren.	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	
	Maatregelen Instelling	**Maatregelen Leverancier**	**Kans**	**Impact**	**Risicoscore**	
	Richt processen in voor beheren van rollen en monitor de implementatie daarvan (RBAC) Implementeer een centraal systeem voor beheren rechten	Ondersteun een geautomatiseerde koppeling met externe identiteits- en toegangsbeheersystemen	Laag	Zwaar	Laag	Restrisico

Tabel 19-12, Verlies van vertrouwelijkheid door handmatige RBAC

Mitigerende actie Xedule	Tijdlijn
Informeren 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	
	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	Restrisico

Tabel 19-13, Verlies van vertrouwelijkheid door onduidelijke configuratiewijzigingen

Mitigerende actie Xedule	Tijdlijn
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	
	Maatregelen Instelling	**Maatregelen Leverancier**	**Kans**	**Impact**	**Risicoscore**	Restrisico
	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	

Tabel 19-14, Verlies van vertrouwelijkheid door Xedule rest API

Mitigerende actie Xedule	Tijdlijn
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	
	Maatregelen Instelling	Maatregelen Leverancier	Kans	Impact	Risicoscore	Restrisico
	De SOAP API koppeling uitfaseren	Ondersteuning van de SOAP API uitfaseren	Laag	Zwaar	Laag	

Tabel 19-15, Verlies van vertrouwelijkheid en controle door ongeautoriseerde toegang door verouderde SOAP API

Mitigerende actie Xedule	Tijdlijn
Uitfaseren 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	
	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	

Tabel 19-16, Heridentificering van gepseudonimiseerde gegevens door gebrekkige anonimiseringsmethode

Mitigerende actie Xedule	**Tijdlijn**
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
18.17	Onduidelijkheid over pseudonimiseringsmethoden	Heridentificering persoonsgegevens betrokkenen	Waarschijnlijk	Enige	Hoog	
	Maatregelen Instelling	**Maatregelen Leverancier**	**Kans**	**Impact**	**Risicoscore**	Restrisico
	Maak gebruik van de opt-out zolang er geen opt-in mechanisme is	Verander het mechanisme naar opt-in	Laag	Enige	Laag	
	NIEUW Informeer medewerkers over het feit dat Xedule contact kan opnemen met de instelling naar aanleiding van hun reacties op de pNPS-uitvraag.	Implementeer aantoonbare maatregelen om heridentificatie te voorkomen				

Tabel 19-17, Heridentificering gepseudonimiseerde pNPS-gegevens

Mitigerende actie Xedule	**Tijdlijn**
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	
	Maatregelen Instelling	**Maatregelen Leverancier**	**Kans**	**Impact**	**Risicoscore**	Restrisico
	Gebruik maken van de read access logs wanneer nodig	Read access logging implementeren	Laag	Zwaar	Laag	

Tabel 19-18, Verlies van vertrouwelijkheid door door ontbreken 'read access logging'

Mitigerende actie Xedule	Tijdlijn
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

Verlies van controle door verplichte openbaarmaking of onbevoegde toegang in derde landen						
Referentie	**Aanleiding**	**Gevolg**	**Kans**	**Impact**	**Risicoscore**	Huidig risico
18.19	Verplichte openbaarmaking en onbevoegde toegang in derde landen	Verlies van controle	Laag	Zwaar	Laag	
	Maatregelen Instelling	**Maatregelen Leverancier**	**Kans**	**Impact**	**Risicoscore**	Restrisico
	Een periodieke beoordeling van de geopolitieke situatie om vast te stellen of de risicobeoordeling moet worden aangepast en een alternatief doorgiftemechanisme moet worden ingezet.	Een periodieke beoordeling van de geopolitieke situatie om vast te stellen of de risicobeoordeling moet worden aangepast en een alternatief doorgiftemechanisme moet worden ingezet.	Laag	Zwaar	Laag	

Tabel 19-19, Verlies van controle door verplichte openbaarmaking of onbevoegde toegang in derde landen

Conclusie

Bij zeventien van de originele risico's waren er maatregelen geïdentificeerd die Xedule moest treffen. Xedule heeft de maatregelen bij elf van deze zeventien risico's uitgevoerd, waardoor tien hoge risico's naar laag zijn gemitigeerd en één risico medium is geworden, mits instellingen ook hun maatregelen uitvoeren. Hiermee blijven er zes hoge risico's over die instellingen niet zelf naar laag kunnen mitigeren. Daarnaast is er één risico dat al medium was en één nieuw laag risico.

Xedule blijft werken om de hoge risico's te mitigeren en heeft nieuwe deadlines vastgesteld. In 2027 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: appId	# 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 Testscenario'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 4.1.
- 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 4.1.
- 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 4.1.
- 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 “bruinr_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 4.1.
- 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 4.1.
- 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 4.1.
- 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 4.1.
- 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 4.1.
- 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 4.1.
- 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 Testscenario's zomer 2026

- Login proces – admin/roosteraar
- Login proces – docent
- Wijzigingsredenen
- Beschikbaarheid motivatie
    - Manager
    - Roosteraar
    - Docent
- Import Templates
- Bewaartermijnen
- Instellingen en autorisaties
- Vrij rondklikken door Xedule en MyXedule

20.4 Voorbeeld inzageverzoek

Zie volgende pagina.

Identiteitsverificatie

Selecteer de van toepassing zijnde betrokkene:

☐ Regulier account
☐ Testaccount of onderzoekaccount

Details Verificatie

Voor Test- en Onderzoeksaccounts
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

Persoonsgegeven	Categorieën betrokkenen	Categorie persoonsgegevens	Gevoeligheid persoonsgegeven	Bron	Onderwijsplanning	Roostering	Authenticatie/identificatie	Backup en gegevensherstel	Personalisering van dienstverlening	Klantondersteuning	Verbetering van de applicatie	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							
Hoofdteam of onderwijsteam	Docent, Medewerker	Organisatiegegevens	Gewoon	HR-systeem / systeem / import	X							
Contracttype (Type arbeidsovereenkomst (Bepaal	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 p	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 Architectuur[54] (HORA) en het Middelbaar Beroeps Onderwijs Referentie Architectuur[55] (MORA). Deze processen zijn daaronder uitgeschreven conform deze referentie architectuur.

HORA	MORA
Onderwijsplanning	
Onderwijsadministratie	Maken jaarplanning
Onderwijseenheidsinschrijving	Aanmelden geroosterde activiteit
Toetsinschrijving	
Vraagprognotisering	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

[54] https://hora.surf.nl/index.php/Hoofdpagina

[55] https://mora.mbodigitaal.nl/index.php/Hoofdpagina

Voor deze verwerking relevante processen beschreven in HORA[56]

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.

Vraagprognotisering:
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 geprognotiseerde 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.

[56] 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 MORA[57]

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

[57] 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, faciliteitengegevens 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 faciliteitenaanbod en het personeelsbestand.